EXHIBIT Q

NETRANGER™

USER'S GUIDE

Version 1.2

Copyright © 1997 by WheelGroup Corporation

WheelGroup corporation

WheelGroup Corporation has made every effort to ensure that this *User's Guide* is correct and accurate, but reserves the right to make changes without notice at its sole discretion at any time.

The NetRanger System described in this guide is supplied under a license and may be used only in accordance with the terms of such license, and in particular any warranty of fitness of WheelGroup Corporation products for any particular purpose is expressly excluded and in no event will WheelGroup Corporation be liable for any consequential loss.

CONFIDENTIAL. The NetRanger System software is confidential and a trade secret of WheelGroup Corporation. All use, disclosure, and/or reproduction of this software not expressly authorized in writing by WheelGroup Corporation is prohibited. WheelGroup Corporation shall prosecute all unauthorized use, disclosure, and reproduction of this software under the criminal and civil laws.

NetRanger, *WheelGroup Corporation*, and the *WheelGroup* logo are trademarks of WheelGroup Corporation. All other product names in this publication are trademarks or registered trademarks of their owners.

Copyright © 1997 by WheelGroup Corporation

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

Produced in the United States of America.

Getting Help

WheelGroup Technical Assistance

Refer to this *User's Guide* whenever you have a problem using the NetRanger System. If you still cannot solve the problem or if you have questions about anything not covered in this guide, you can call WheelGroup Technical Support from 8:00AM to 6:00PM, CST. This assistance is available Monday through Friday (except holidays). You can reach us in any of the following ways:

Telephone	**1-888-942-6762**
FAX	**210-494-6303**
E-Mail	**help@wheelgroup.com**

Please include the following information in your FAX or e-mail message, or have it available if you are calling (Use the NetRanger Problem Report Form on the following page to help you gather this information.):

- Your customer number and phone number. For e-mail messages, please include your customer number as part of the subject line for your messages.
- A description of the NSX and Director hardware and software you are using, including any network software.
  Note: To determine the version number of the Director software you are using, type the following command:
  ```
  nrdirmap -?
  ```
- Your operating system type and version
- A description of the problem, what you were doing when it occurred, and the exact wording of any error messages that you might have received.
- If this is a security question, please include all information related to a specific alarm or attacking site.

NetRanger Problem Report Form

Before you call, please have the following information available.

Organization ID:____________________ Host ID (of Problem System):____________________

Point of Contact:____________________ Phone Number:____________________

For Director or NSX Problem

NSX Information (if applicable)

NSX Type:____________________ Number of NSC devices connected to NSX:__________

NSC Type (with problem):____

NSC Serial Number (with problem):____

Director Information (if applicable)

Platform: HP SPARC

OV Version:____________________ Director Version:____________________

Problem Description

____

____

____

____

____

For Security Incidents

Are you a monitored site? Yes No Member of WARN? Yes No

IP addresses of involved machines:____

Do you wish to talk to WheelGroup about
Intrusion Control and Response (ICR) consulting? Yes No

Alarm Type:____________________

Description of security incident:____

____

____

WheelGroup Corporation
1-888-942-6762
1-210-494-6303 (fax)
e-mail: help@wheelgroup.com

Table of Contents

I Overview

NetRanger's Components and Capabilities

What is NetRanger?

NetRanger is a real-time network security management system that detects, analyzes, responds to, and deters unauthorized network activity. The NetRanger architecture supports large-scale information protection via centralized monitoring and management of remote dynamic packet filtering devices that plug into TCP/IP networks. Communication is maintained via WheelGroup Corporation's (WGC) proprietary secure communications architecture. Network activity can also be logged for more in-depth analysis.

As shown in Figure I-1, NetRanger 1.2 consists of the following core systems and subsystems:

- **Network Security eXchange (NSX)**
  - ◊ Packet Filtering Device(s)
  - ◊ Sensor
- **Communications System**
  - ◊ Post Office(s)
  - ◊ Encrypted Sleeve
- **Director**
  - ◊ Security Management Interface
  - ◊ Security Analysis Package

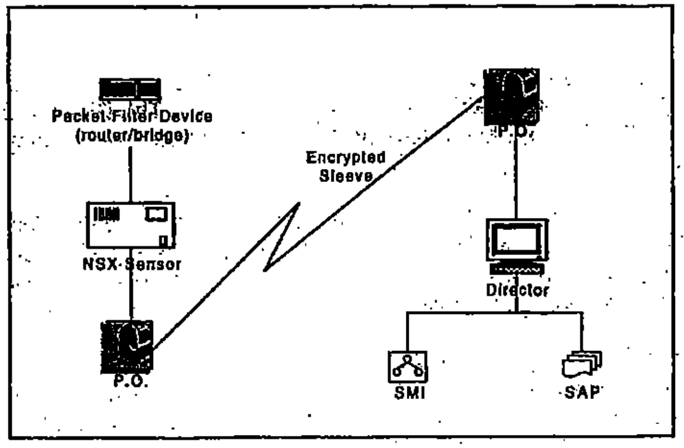


Figure I-1: Basic NetRanger Components

The NSX

The NSX is the on-site filtering, sensing, and management component of the NetRanger System. It communicates with one or more remote Director systems via the Post Office network communications system. The NSX currently operates with IP networks and supports many hardware and software configuration options.

The Packet Filtering Device is a router or bridge that plugs into a network at a point of entry to other networks. The security policy installed on this device determines what subset of network traffic will be routed to the NetRanger Sensor.

The Sensor subsystem contains NetRanger's real-time intrusion detection and content assessment logic. The intrusion detection engine recognizes and responds to attacks, such as sendmail, ping sweeps, IP source routing and spoofing, FTP and Telnet abuse, and SATAN scans. Sensor analyses produce data streams of IP packets and event records that are either dumped into local session log files or sent on to the Post Office for remote delivery to a Director system. The Sensor also accepts intrusion response and reconfiguration information from Director systems.

The Communication System

The Post Office subsystem provides remote monitoring and NSX systems management. All communication is based on a proprietary, connection-based protocol that can switch between alternate routes in order to maintain the point-to-point connections specified in its routing tables. All messages are routed based on a three-part address that includes organization, host, and application identifiers.

The Encrypted Sleeve secures data transmission between remote protected networks. Encrypted sleeves are currently implemented via the Data Privacy Facility (DPF) that comes with Network System Corporation's (NSG) BorderGuard packet filter devices.

The Director

The **Director** provides monitoring and analysis services to NetRanger, and communicates with one or more NSX systems via the communication system. The Director contains two basic subsystems: the Security Management Interface (SMI) and the Security Analysis Package (SAP).

The SMI is a collection of GUIs and tools that help monitor and respond to security events at one or more NSX locations. The SMI integrates with network management applications (such as HP OpenView™) via menu add-ons. Whereas the SMI is focused primarily on real-time security event management, data analysis is supported by the SAP.

The SAP is a set of data analysis tools that analyzes NSX data independently of SMI activities. The SAP consists of two basic components: database export utilities to relational databases (such as Oracle™) and one or more data analysis tools. Both types of components can be easily integrated into an existing SMI platform. However, WheelGroup Corporation recommends that all data be exported onto a separate host. In this way, the SMI and SAP components can be configured, secured, and tuned independently.

Product Capabilities

NetRanger integrates many tried and true network security technologies which makes it the preeminent intrusion detection system. Most network security applications fall into one of two categories: **firewalls or network monitoring.** Both of these technologies suffer from shortcomings not found in NetRanger.

Firewalls represent the most common form of network security, and they gained popularity in part because of their relatively simple host-based installation and friendly graphical user interfaces. The biggest problem with firewalls, however, is that they rely upon *proxy services* to enforce an organization's security policies. Proxy services erect *static* barriers that frequently block legitimate as well as illegitimate activity. This puts pressure on system administrators to open pathways, which makes firewalls vulnerable to the very events they are supposed to guard against. Because most firewalls are host-based solutions, administration of more than one firewall at a time is also difficult. The system overhead associated with proxy services also prevents most firewalls from being able to scale beyond Ethernet speeds.

Although network monitoring tools can detect unauthorized activities without having to erect barriers to entry, administrators typically have to sift through audit logs after the fact in order to find security breaches. In many instances, systems have been compromised by the time the activity has been detected. Both of these approaches also tend to only look at incoming network traffic.

NetRanger enforces an organization's security policy via **real-time response and detection of intrusive events** without having to erect static barriers. NetRanger's secure communication architecture also allows command and control, as well as system information, to be distributed across secure networks. This section describes these capabilities in a top-down fashion within the context of the underlying architecture.

One of the fundamental design principles of NetRanger is that the *services* required by each of the subsystems be broken apart into their atomic operational components, or *daemons*, which are diagrammed in Figure I-2. For example, the NetRanger daemon that logs events is totally separate from the ones that perform network sensing and device management. The reasons for this approach are **speed, durability, scalability,** and **independence.**

Each of NetRanger's daemon services is purpose-built for a specific task. This makes it possible to optimize each service without compromising the functionality of the other services. Purpose-built components also tend to be more durable than systems that manage multiple tasks, and are easier to debug and upgrade.

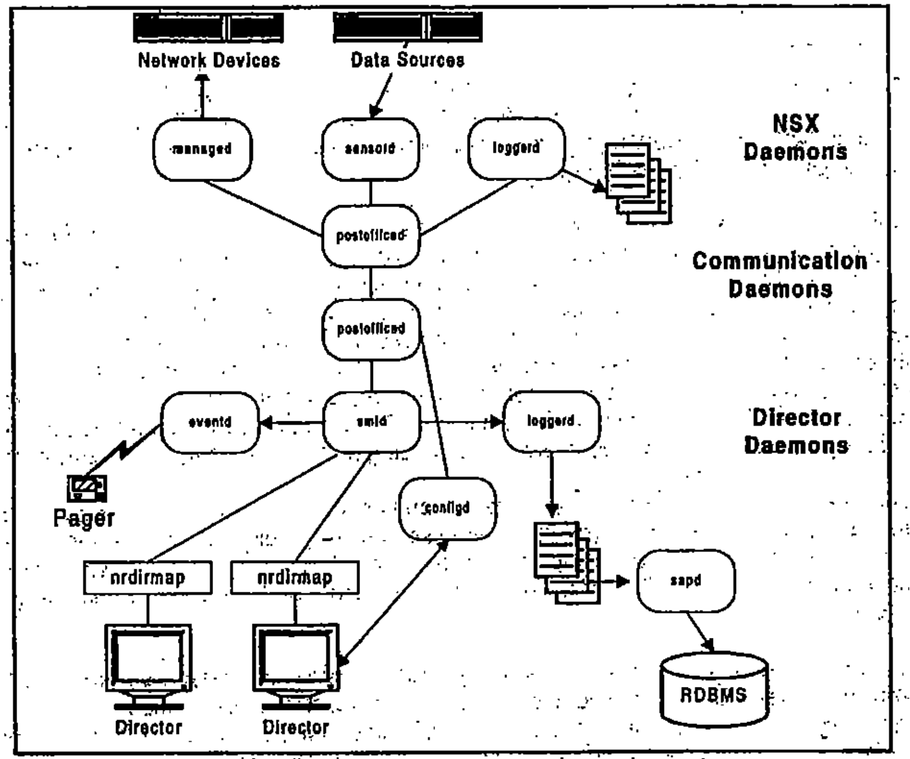


Figure I-2: NetRanger 1.2 Architecture

NSX System

The NSX's capabilities are best described as **network sensing, device management,** and **session logging,** implemented respectively by the *sensord, managed,* and *loggerd* daemons diagrammed in Figure I-2.

Although NetRanger is frequently described as an *Intrusion Detection* system, it also looks for a variety of suspicious activities that precede unauthorized events. An NSX will detect and report a ping sweep of a network. Although not truly intrusive, a ping sweep is frequently a precursor to unauthorized activity. The NSX system therefore looks for network **patterns of misuse** based on a variety of different **attack signatures.**

Network Sensing

Patterns of misuse are identified by two basic types of network signatures: **context** and **content.** Context-based signatures deal with the *state* of a transmission as defined by the structure of packet headers, and content-based signatures focus on *what* is being transported—the binary data. Context-based signatures tend to be more complex than content-based ones and the steps required to identify them are also complex and proprietary. As a consequence, context-based signatures are embedded within the NSX sensor subsystem, whereas content-based signatures are configurable and can be added dynamically at runtime.

Network Protocols

The sensor subsystem currently works with **TCP/IP**. Future releases of NetRanger will support other network protocols, such as Novell's IPX/SPX.

Packet Filter Devices

The only type of packet filter devices the sensor subsystem currently works with are the **BorderGuard** and **Passport** devices from Network Systems Group (NSG). These packet filter devices play a key role in the success of the NSX system.

In addition to serving as high-speed IP data sources, all of these devices

- can be **reconfigured on the fly**,
- support the same **NetSentry interface**,
- can be deployed as **bridges** as well as **routers**, and
- can maintain **Virtual Private Network** (VPN) connections.

Because these devices can be reconfigured on the fly, NetRanger can dynamically **shun as well as detect** suspicious and unauthorized network activity. The common command and control interface provided by NetSentry allows one NSX to support all three devices. Please note that these devices can operate as bridges as well as routers, which means that an NSX can be deployed in a network behind existing devices, such as Cisco routers, without having to change routing protocols or reassign existing network addresses. Finally, the VPN facilities provided by NSG are the key to NetRanger's secure communication system.

Performance Capabilities

The NSG packet filter devices fall into three distinct price/performance products: the BorderGuard 1000, BorderGuard 2000, and the Passport. These packet filter devices serve as the basis for the three NSX configurations currently offered by WheelGroup: the NSX 1000, 2000, and 5000 systems. As with the NSG systems, the primary difference between the NSX systems is one of network performance, which is summarized in Table I-1. For detailed hardware information on any of these systems, refer to Appendix D in this *User's Guide.*

	NSX 1000	NSX 2000	NSX 5000
Max Bandwidth	512 Kbps	T1 (or 10 Mbps)	T3 (or 100 Mbps)
NSG Device	BorderGuard 10000 > 2 Ethernet > 3 WAN/1 Ethernet	BorderGuard 2000 > 4 Ethernet > 2 Ethernet/2 WAN	Passport > FDDI > Ethernet > WAN > Token Flag
NSX Sensor	Pentium 166 Mhz > 2 GB Hard Drive > 32 MB RAM > 10BaseT Ethernet > modem dial-up > 2 serial ports	Pentium 166 Mhz > 2 GB Hard Drive > 32 MB RAM > 10BaseT Ethernet > modem dial-up > 2 serial ports	UltraSPARC 170 Mhz > 4 GB Hard Drive > 64 MB RAM (min) > SBUS FDDI > modem dial-up > 2 serial ports

Table I-1: NSX Configurations

NetSentry

As noted earlier, NSX Intrusion detection is based on the **monitoring of an open network connection rather than a closed one.** The NSX does this by leveraging the layered filter architecture built into NetSentry, which is diagrammed in Figure I-3.

The *First*, *Apply Table*, and *Last* filter points apply to **all** of the network interfaces installed on a BorderGuard/ERS system, whereas the *Incoming* and *Outgoing* filter points allow different **in** and **out** policies to be applied to each of the network interfaces installed on the device.

One of the reasons the NSX system is able to perform **real-time** intrusion detection is because it is able to leverage the **copy_to/log_to** auditing features via filters applied to the *First* filter point. For example, the NSX's default *first.fil* filter instructs the BorderGuard/ERS to only pass on specific IP packets to *sensord.* This helps to dramatically reduce the amount of traffic the NSX system has to process.

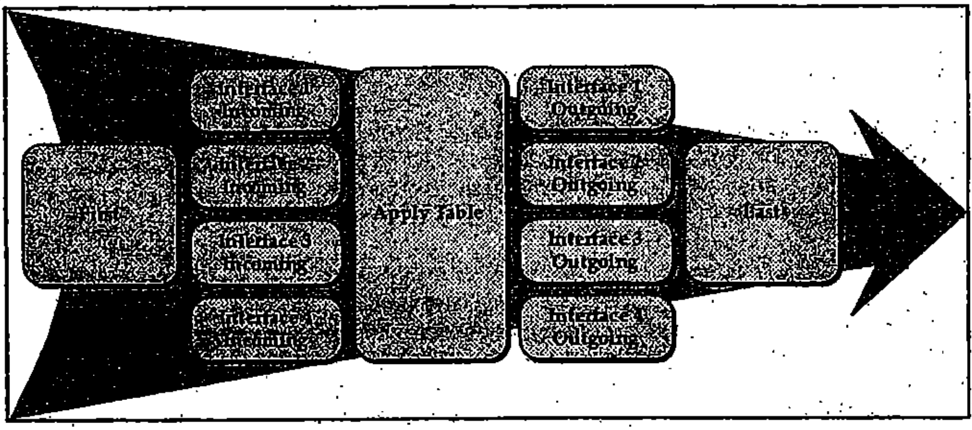


Figure I-3: NetSentry PCF Filters

Attack Signatures

As previously mentioned, an attack signature is a *pattern of misuse* based on one or more events. Such a pattern can be as simple as an attempt to access a specific port on a specific host, or as complex as sequences of operations distributed across multiple hosts over an arbitrary period of time. Events can be grouped into different *attack signatures*. An event that is based on a single ICMP packet at a specific point in time is an **atomic signature** (e.g., a ping of a specific host). **Composite signatures**, on the other hand, are based on series of events. A ping sweep is an example of a signature that spans a network; a port sweep is an example of a signature that focuses on a specific host. A SATAN attack is an example of a composite signature derived from a host port sweep pattern. Many of these patterns are also *stateless*, which means that the attack signature must be identified regardless of the order or the duration between atomic events. Other signatures, such as SYN attacks, are based on well-defined event sequences that are *stateful*.

Attack Responses

The NSX system does one or more of the following things once an attack has been positively identified:

- **Generate an alarm**
- **Shun the attack**
- **Log the alarm event**

In keeping with the flexibility of NetRanger, the initiation of these actions, as well as how they are initiated, is highly configurable.

Alarms

Alarms are generated by the *sensord* daemon, and are typically routed to a remote Director system. These notifications can also be routed to **multiple** Director systems.

The type of alarm generated for a specific attack is dictated by configuration tokens stored in the NSX configuration file /usr/nr/etc/sensord.conf. Alarm notifications are grouped according to their **severity of misuse.** You can define up to 255 different levels of severity. However, NetRanger's default configuration currently specifies 6 levels of misuse.

Shunning

In addition to generating alarms, *sensord* can initiate **optional actions.** The most common action is to **shun an attack,** which typically involves reconfiguration and reloading of the NetSentry *Apply Table* (as diagrammed in Figure I-3). This type of automated response should only be configured for attack signatures with a low probability of a *false positive* response. A SATAN attack is an example of an unambiguous activity, whereas a content-based signature such as "VRFY" (off mail port 25) is more prone to a false positive pattern match.

Another way of shunning patterns of misuse is to manually reconfigure the BorderGuard or Passport device through the Director system. Shunning is part of a site's security policy that must be carefully reviewed before it is deployed, whether as a set of automatic rules in sensord.conf, or as a set of guidelines that operational staff rely on.

Logging

All NSX log data is written to **flat files,** which can then be exported to industrial-grade databases by the SAP subsystem described in the *Director* section. Data is written directly to flat files instead of a database in order to maximize **fault tolerance** and **performance.**

The NSX system currently supports two types of logging:

- **Event logs**
- **IP Session logs**

Alarms represent just one type of *event* that can be logged by the NSX system. Event logs can also contain entries for every *command* and *error* that is generated by a user or daemon service. Data is written to these type of log files as long as NetRanger is running. Log files are **serialized** based on configurable time and size intervals defined in /usr/nr/etc/loggerd.conf. The naming convention for Event log files is **log.<date-time>.**

IP Session logs are only written to when a certain event(s) occurs, such as a connection request from a specific IP address, or detection of a string such as "Confidential." When these type of conditions are met, *sensord* can be configured to write every incoming and outgoing packet to an IP Session log for a predefined period of time. IP Session logs allow you to reconstruct the *conversation* that takes place between a source and destination IP addresses. The naming convention for IP Session logs is **log.<src IP address>.**

ERRORS

Data Type:	2
Record ID:	1000002
GMT Timestamp:	839348960
Local Date:	1996/08/06
Local Time:	11:29:20
Appl ID of Source:	10000
Host ID of Source:	3
Org ID of Source:	100
Error Message:	Network failure for connection 1 to destination [1.100]

EVENTS

Data Type:	4
Record ID:	1108957
GMT Timestamp:	839450792
GMT Date:	1996/08/07
GMT Time:	15:46:32
Appl ID of Source:	10001
Host ID of Source:	1
Org ID of Source:	100
Location of Source Address:	OUT
Location of Destination Address:	IN
Level of Event:	2
Event Signature:	10000
Event Sub-Signature:	1007
Protocol:	TCP/IP
Source IP Address:	129.210.8.1
Destination IP Address:	10.3.55.125
Source Port:	1956
Destination Port:	23
NSG Router Address:	10.3.55.200
Optional String:	incom1_telnet_fail

COMMANDS

Data Type:	3
Record ID:	1000003
GMT Timestamp:	839479664
Local Date:	1996/08/07
Local Time:	23:47:44
Appl ID of Source:	10005
Host ID of Source:	3
Org ID of Source:	100
Appl ID of Requestor:	10002
Host ID of Requestor:	3
Org ID of Requestor:	100
Command:	GET FilenameOfConfig

Figure I-4: Event Log Formats

Timestamp	Packet Length	IP Packet
4 bytes	4 bytes	20+ bytes

Figure I-5: IP Session Log Format

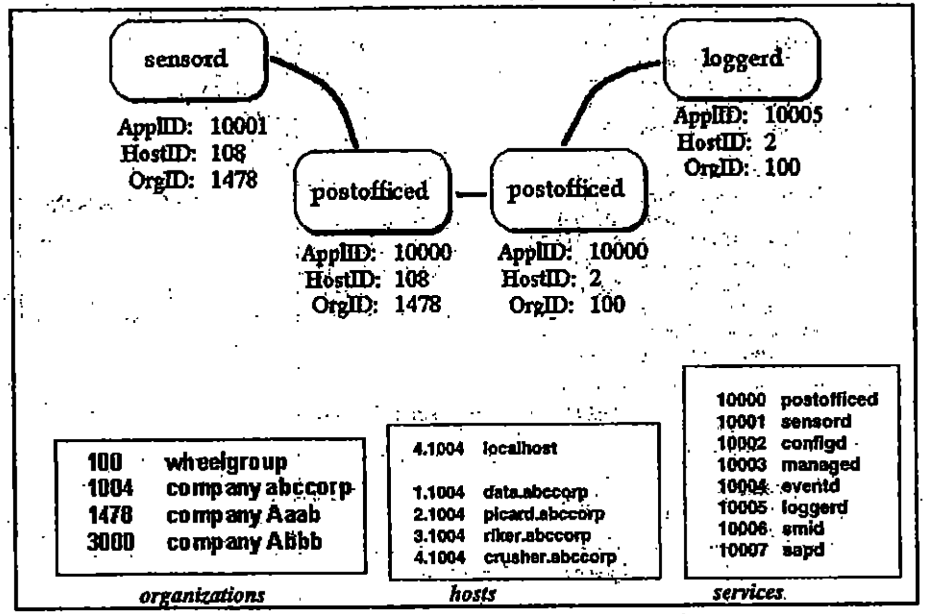
Note that both Event and IP Session information can be logged locally on the NSX system as well as remotely on Director systems; exactly **what** information is sent **where** depends on how each NSX system is configured.

Communications System

NetRanger is a **distributed application** that allows exchange of audit information and command and control across networks. All communication is based on a **proprietary, connection-based protocol** that is **fault-tolerant** and supports **alternate routes.** Although the communication system currently only runs on top of TCP/IP networks, it has been implemented at the **application layer** of the OSI network model to eventually operate on top of other protocols, such as IPX/SPX and NetBios. The underlying packet transfer mechanism employs a **sliding window** for performance and is **UDP-based** for scalability.

Communications Protocol

As Figure I-6 illustrates, all of the NetRanger daemons communicate with one another via *postofficed* daemons. Note that this holds true for communication between daemons on the same host as well as across hosts. All communication is based on a unique three-part address that includes **Organization, Host,** and **Application** identifiers, which are enumerated in each NSX's and Director's *organizations, hosts,* and *services* files in /usr/nr/etc.



100	wheelgroup
1004	company abccorp
1478	company Aaab
3000	company Abbb

4.1004	localhost
1.1004	data.abccorp
2.1004	picard.abccorp
3.1004	riker.abccorp
4.1004	crusher.abccorp

10000	postofficed
10001	sensord
10002	configd
10003	managed
10004	eventd
10005	loggerd
10006	smid
10007	sapd

Figure I-6: Example /usr/nr/etc communication files

The benefits of this proprietary addressing scheme are twofold: 1) it can be layered on top of existing network protocols and 2) it can address a much larger domain than the current 32-bit IP protocol.

Alternate Routes

NetRanger's three-part addressing scheme serves as the basis for a point-to-point protocol that allows for up to 255 alternate routes between two hosts. These alternate pathways are defined in /usr/nr/etc/routes, which also maps NetRanger addresses to native host addresses. Figure I-7 shows two alternate routes to the "abccorp" host "data". The preferred path is via an IP host with the address of 10.3.55.151; an alternate path has been identified via a host with an IP address of 10.1.4.198.

```
data.abccorp      1  10.3.55.151      45000  1
data.abccorp      2  10.1.4.198       45000  1
picard.abccorp    1  10.1.4.198       45000  1
```

Figure I-7: Example /usr/nr/etc/routes file

An important feature of this alternate routing protocol is that it automatically switches to the next route whenever the current route fails. It also uses a system heartbeat to detect when a connection to the preferred route can be reestablished. A system error message is generated (and logged) whenever a connection goes down, and any packets that were lost during the state transition are resent.

Distribution of Data

In addition to specifying alternate routes and maintaining fault tolerance, the communication protocol also allows you to define **what** types of information and **how much** information should be sent to each destination.

As noted earlier, the types of information generated by the NSX daemon falls into four basic categories: **Events, Commands, Errors,** and **IP Packets.** The /usr/nr/etc/destinations file allows you to specify what types of information should be routed to which **daemons** on which **hosts.** Figure I-8 shows two different distribution entries. The first entry routes all of the standard Event data to the *loggerd* service on a Director machine named crusher, and the second entry specifies that only *events* should be displayed by *smid* on the riker Director machine.

```
1 crusher.wheelgroup      loggerd   1   EVENTS,ERRORS,COMMANDS
2 riker.wheelgroup          smid     2   EVENTS
```

Figure I-8: Example /usr/nr/etc/destinations file

In addition to specifying what *types* of information should be distributed, NetRanger can dictate what *levels* of event should be sent to each destination. As shown in Figure I-8, only events of level "2" *and above* are being sent to *smid* on *riker.*

Distribution Hierarchies

Another feature that complements alternate routing is the ability to build **hierarchies** of NSX and Director systems through the use of **message propagation.** Instead of broadcasting events from an NSX onto multiple hosts, information can be sent to a single host, which can then propagate packets onto other platforms defined in its local configuration files. Figure I-9 illustrates this concept via a simple hierarchy of Director machines.

In addition to providing a degree of fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9 am to 5 pm and then transfer control onto a central Director every evening.

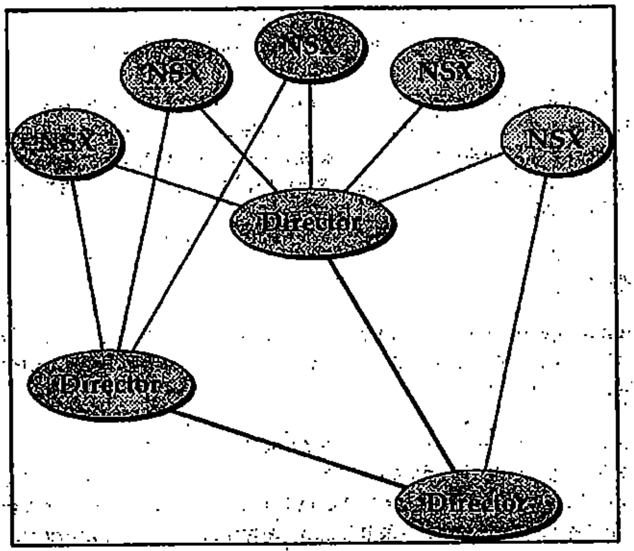


Figure 1-9: Director Hierarchy Based on Message Propagation

Encrypted Sleeves

A key requirement of the communication architecture is its **security,** which is achieved by passing all communication between NSX and Director systems through NSG's Data Privacy Facility (DPF). The DPF maintains Virtual Private Networks **(VPN)** via **RSA** public-key and one of the following private key systems: **DES, Triple DES**, or **IDEA**. The DPF is noteworthy in that

- it can be **maintained across collections** of NSX and Director systems, and
- it is **transparent** to applications such as NetRanger.

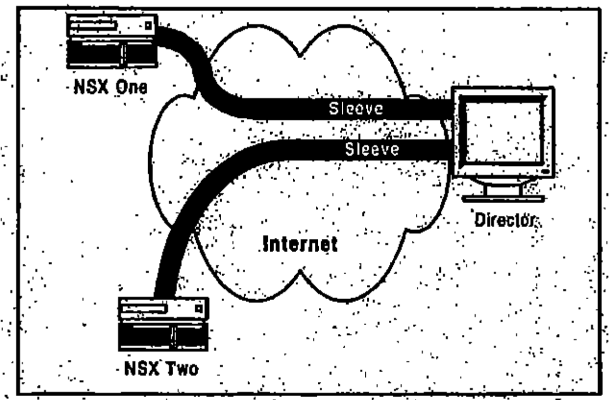


Figure I-10: Example of NSG's VPN

Director System

As noted earlier, the NetRanger Director consists of two major subsystems:

- **Security Management Interface (SMI)**
- **Security Analysis Package (SAP)**

These two subsystems provide **centralized command and control** of an organization's security perimeter, which could conceivably encompass hundreds of NSX systems. From a capabilities perspective, these two subsystems provide **monitoring, management, data collection, data analysis,** and **user-defined actions** services. All of these capabilities are supported by the *smid, configd, loggerd, sapd,* and *eventd* daemons diagrammed in Figure I-2. There is also an application called *nrdirmap* that serves as the interface between *smid* and HP OpenView.

NSX Monitoring

The Director's most prominent capability is display of **real-time** event information, which is based on the *smid* daemon, the *nrdirmap* application, and OpenView. The *smid* daemon accepts incoming event records from one or more NSX systems via a local *postofficed* and translates them into a format that *nrdirmap* understands. The *nrdirmap* application uses the OVW API (OpenView Windows Application Programming Interface) to tell the OpenView user interface what security information to present to the user. Security information is presented via **icons** drawn on one or more **network security maps.** Figure I-11 shows an example of the Director's display of a collection of NSX systems.

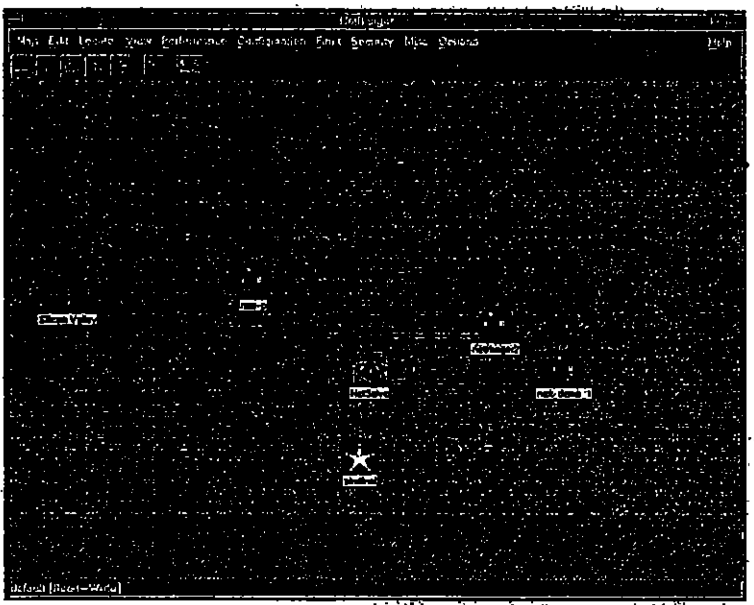

NetRanger
Map Edit Locate View Performance Configuration Fault Security Misc Options
Help

Figure I-11: Example Director Network Security Submap

Network Security Maps

The Director arranges icons into hierarchical security maps based on OpenView's Network Node Management (NNM) user interface. If you double-click an icon, you can view the next lower "submap." Figure I-12 shows several examples of *Event/Alarm* icons. The Director hierarchy includes the following levels, where *NetRanger* is the "root" and *Events/Alarms* are the "leaf" nodes of the tree:

- **NetRanger**
  - **Collections** of Directors/NSXs
    - A Single **Director or NSX** System
      - **Applications** running on a Director or NSX System
        - **Events/Alarms** generated by an Application

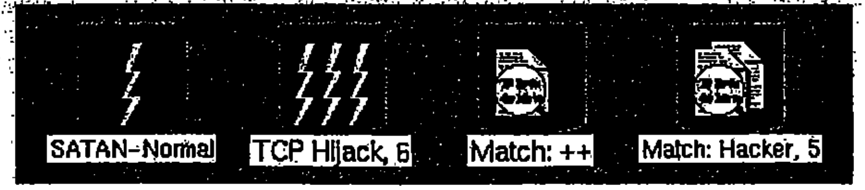


Figure I-12: Sample Director Alarm Icons

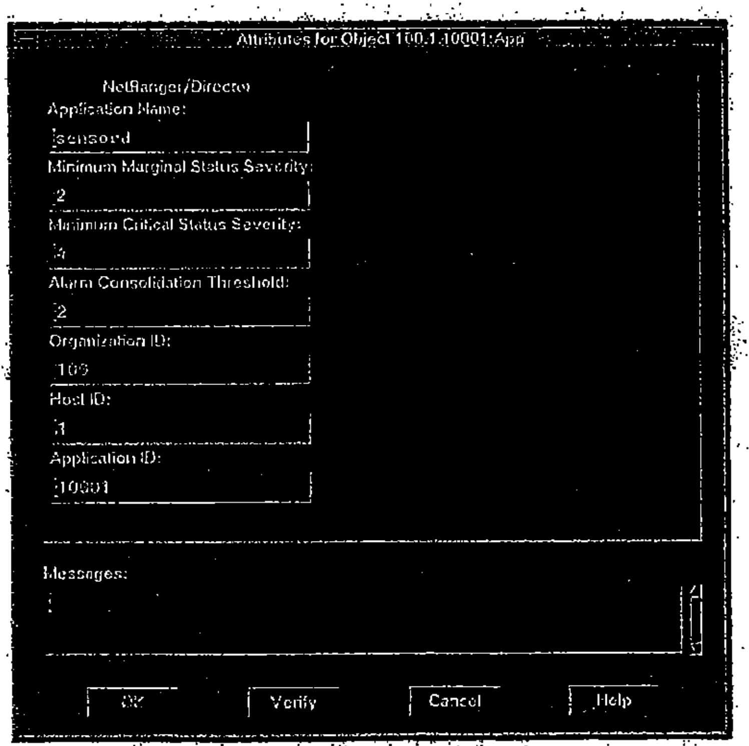
Icon States

Every icon within a network security map has a **state**, which is expressed in the form of textual and graphical attributes.

The most visible indication of an icon's state is its **color**. The colors **green, yellow,** and **red** represent the states **normal, marginal,** and **critical**. These states are user-defined in an attribute dialog (shown in Figure I-13). Level 2 and 3 alarms are usually set as *marginal* (yellow), and level 4 and 5 alarms are set as *critical* (red).

Unlike all other icon attributes, color is a state that is **inherited** from *Event/Alarm* icons by all other levels of the icon hierarchy. For example, an NSX machine icon is automatically set to red if any of its subordinate NSX applications has received a critical alarm. The **ability to propagate** alarm states up through a hierarchy is one of the features that makes the Director such a powerful network security monitoring tool.

Every icon in a Director hierarchy also possesses textual attributes. This information is accessed by selecting a particular icon and then choosing **Describe→Modify** from the menu bar or pressing **Ctrl+O,** which brings the icon's attributes dialog forward. Each type of icon has a different set of attributes. Figure I-13 shows the attributes for an NSX *sensord* icon.



Application Name: sensord

Minimum Marginal Status Severity: 2

Minimum Critical Status Severity: 4

Alarm Consolidation Threshold: 2

Organization ID: 100

Host ID: 1

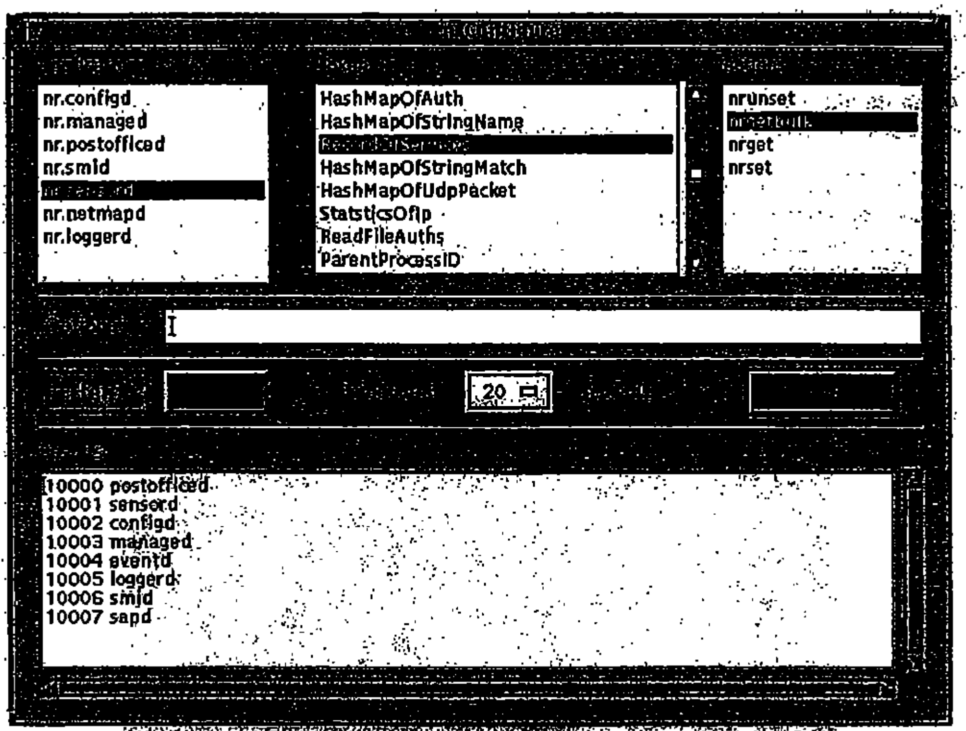
Application ID: 10001

Messages:

Figure I-13: sensord Attribute Information

NSX Management

Another key capability of the Director is remote management of the daemon processes (or *Applications*) that make up an NSX system. *Applications* are managed via a graphical user interface called **nrConfigure**, which talks directly to the *configd* daemon. This interface allows a user to effectively *get* and *set* such attributes as log file names and alarm responses. The nrConfigure interface is activated by selecting one or more icons on the security map and then choosing **Security→Configure** from the OpenView menu. This opens the window shown in Figure I-14.



nr.configd
nr.managed
nr.postofficed
nr.smid
nr.sensord
nr.netmapd
nr.loggerd

HashMapOfAuth
HashMapOfStringName
RecordOfServices
HashMapOfStringMatch
HashMapOfUdpPacket
StatsticsOfIp
ReadFileAuths
ParentProcessID

nrunset
nrgetbulk
nrget
nrset

```
10000 postofficed
10001 sensord
10002 configd
10003 managed
10004 eventd
10005 loggerd
10006 smid
10007 sapd
```

Figure I-14 NSX Configuration Interface

The **Applications** displayed in nrConfigure's top left-hand list box represent the services running on the first NSX icon highlighted by the user. The top center list box displays all of the **Tokens** that apply to the Application currently highlighted in the left-hand list box. The top right-hand list box displays the **Actions** that are allowed for the currently selected Token. Figure I-14 shows the Actions and Tokens for the *sensord* daemon.

NetRanger currently supports over 100 tokens. An *Action* is put into effect by pressing the **Execute** button. The five possible actions are **get**, **getbulk**, **set**, **unset**, and **exec**.

The **get** and **getbulk** commands are read-only operations that obtain information from an *Application*. The **get** command returns a *single* item of information; **getbulk** returns a *set* of items. Figure I-14 shows the results from a getbulk request for all of the services defined for an NSX or Director.

The **set** command is a write operation that updates the value of a *Token*; **unset** removes a specific Token and its value from an Application's configuration. Adding or deleting a content-based attack signature (such as "VRFY") from an NSX is one example of these *Actions*.

The **exec** command instructs an application to execute an action external to itself. For example, you can instruct an NSX to shun a specific IP address by issuing an **exec** against *managed*, which in turn modifies the filter configuration on its packet filter. The **exec** command is also used for such tasks as writing configuration information to disk.

It is important to understand that all configuration data is read and written to or from the *Applications* themselves, not from local caches or parameter files. The results of a **set** or **exec** take effect immediately on the target NSX.

Finally, all of the functionality provided by nrConfigure is also available via command-line interfaces. This allows trusted users without access to a Director to manage NSX systems from a simple terminal session.

NSX Data Collection

NSX data collection serves as the foundation for the SAP subsystem, and is based on the *loggerd and sapd* services diagrammed in Figure I-15. These daemons use a simple **push-pull** mechanism to migrate data into a remote database. As explained earlier, *loggerd* pushes data into flat files, which are serialized based on configurable size or time thresholds. This data is then pulled into a remote database by *sapd*, which has its own polling interval.

Writing to intermediate flat files in this manner provides levels of **fault tolerance** and **performance** cannot be achieved when writing directly to a database. Data throughput in a distributed application such as NetRanger is constrained by the weakest link in the system.

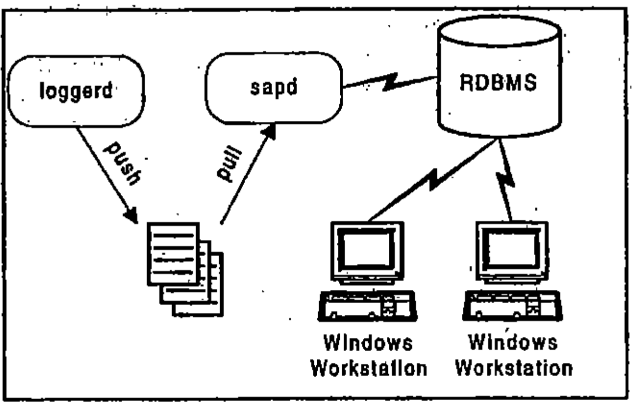


Figure I-15: NSX Data Collection

With the SAP system, the data capture process is insensitive to database availability or performance fluctuations.

The SAP currently ships with *sapd* drivers for **Oracle**® and **Remedy**®. However, SAP can also be configured to write to other databases, such as Sybase® and Informix®. Example scripts are shipped with the Director that show how a database's native bulk load tools can be easily integrated into *sapd.*

NSX Data Analysis

The SAP capability also analyzes data. Rather than locking the user into a single tool on the Director machine, this task is better served by **third-party tools** on a separate Windows platform, such as the IQ Objects® **report writer** from IQ Software and **multi-dimension analysis** tools such as PowerPlay® from Cognos. **Trouble ticketing** systems such as Remedy's Action Request System® (ARS) can also be implemented on top of NetRanger's alarm data.

These type of third-party tools can be configured to support ad hoc queries as well as predefined reports. For example, these tools can easily generate reports showing

- all alarms of levels 4 and 5 in the last 30 days,
- a graph of Web server activity over the last 24 hours, and
- a table of all events in the last 30 days in order of increasing alarm levels.

User-Defined Actions

In addition to displaying and logging alarm events, the Director can generate user-defined actions via *eventd.* A typical action might be to generate pager notifications via e-mail, or feed data onto third-party devices, such as a printer. Support for multiple action scripts is also provided. While *eventd* makes no distinction between alarm types and levels, the default action script shipped with this service shows how actions can be triggered based on these criteria.

NSX

Bridge Mode

With the 4.0 release of Network System Group's NetSentry operating system, NSX systems can now be deployed in a bridge configuration. The primary benefits to this type of deployment are described in Chapter II of the *User's Guide*, and can be summarized as follows:

- NSX systems can be deployed in established networks without having to alter existing network configurations or equipment.
- Bridge mode implementations are invisible on the network. They are effectively *bumps on the wire.* They have a single IP address that can be hidden through effective security filters.

Alarm Context Streams

An NSX sensor can now be configured to capture the incoming and outgoing network traffic that precedes a content-based alarm (SigIds: 3100-3104, 3200, 3201, 8000). This information can be used to reconstruct the events that led up to the event. Each data stream is currently limited to 256 bytes of information. Corresponding enhancements have been made to the Director *display* and SAP functions to accommodate this new type of information.

New Signatures

Refer to Chapter IV for a listing of new signatures.

Network Device Auto Detection

An NSX now automatically identifies the type and version of packet filter it is connected to, and adjusts its interfaces according to the operating system version [(v3) with PCF versus (v4) with NetSentry] as well as the type of device (BorderGuard versus Passport).

Bug Fixes

Multiple Shuns

managed has been written from the ground up. Now you can not only shun a host, but also a network, and unshun a host, unshun a network and unshun all. Additionally, commands can be sent through the nrConfigure interface. When using nrConfigure, users can select *managed,* and then select Help to read a FAQ on *managed* enhancements.

Communication

Bug Fixes

Unexplained loss of information from a remote system
Occasionally, 1.1 versions of the Director would lose the ability to send or receive information from an NSX. The problem would manifest itself in one of the following ways:

- The Director would stop displaying alarms and log events from a specific NSX.
- nrConfigure returns with a timeout error for all nrset/nrget actions against that NSX.

These symptoms made no sense because the utility /usr/nr/bin/nrconns (which performs a nrgetbulk on "DestinationConnectStatus" on all of the hosts listed in /usr/nr/etc/hosts) always showed the NSX as having a normal "[Established Connection]" status. This problem always disappeared when the underlying NSX daemons were stopped and restarted.

Testing ultimately showed that this problem arose when an NSX system's *postofficed* was restarted before the heartbeat interval on the Director system had timed out (at 20 seconds). The Director system failed to detect that the connection was lost because the restarted NSX system sent an ACK back to the Director before it initiated its next heartbeat. Consequently, the Director never sends a SYN packet to reestablish the connection's (NextRecvMsg) sequence number. The restarted NSX restarts with a NextRecvMsg sequence number of "0" while the Director continues to look for a non-zero sequence number based on the last successful communication with that NSX system. This causes the Director to discard all subsequent messages from that NSX.

This problem has been fixed by having a system, whether it is an NSX or a Director, not respond to a remote postoffice's heartbeat request until it receives a SYN packet from that remote system's postofficed. In turn, a remote postoffice automatically resynchs when its heartbeat process timeouts for a remote system.

Director

Alarm Context Streams Display

The Director has been enhanced to display the alarm context information that an NSX can now associate with a given alarm. This information is displayed in a split window that shows the incoming data stream in one window and the outgoing data in the other. Non-printable characters (such as carriage returns and line feeds) are displayed in an ASCII hexadecimal format. This type of information is accessed via the **Security→Show→Context** menu option.

Null Machine Icons

In the 1.1 version, users could incorrectly add a symbol, resulting in nrdirmap generating errors. Now, added error checking capabilities will automatically delete improperly added icons.

Improved Shun Capability

Users now have the ability to shun individual hosts and class C networks by clicking on an alarm and selecting either **Security→Shun→Source IP or Security→Shun→Source Net.**

New Icons

New application icons were created for *sensord*, *sapd*, *configd*, and *loggerd*.

Copyright Information

The **Security→About** window has been changed to display copyright information.

SAP Enhancements

loggerd failsafe features
loggerd now has two failsafe features, one to protect against runaway serialization during heavy network traffic, and the other to keep files from being overwritten due to constant starting and stopping of processes.

NSX Log File Management
In addition to processing Event logs on a Director system, the SAP package has been enhanced to manage log files on an NSX system. Users can now configure an NSX to automatically process an NSX system's IP Session log files as well as its Event logs. In addition to making it easier to manage an NSX's file system, this enhancement makes it easier to retrieve NSX log files from a Director system. While the default *sapd* action on an NSX system is to compress and archive files to tape, it could be configured to ftp these files to another host, or spool the data to a print server.

sapr
The SAP package now includes a set of SQL queries that generate simple columnar reports. Although these queries generate useful information, their primary purpose is to demonstrate how event data can be analyzed relative to the three primary *dimensions* implicit in the data: *time*, *space*, and *event*.

nrConfigure Comes Up Faster

The 1.2 version of nrConfigure performs much faster than its predecessor. Whereas the 1.1 version could take up to 20 seconds to appear on the screen, the 1.2 version rarely takes longer than three seconds to appear.

Bug Fixes

No Director Icon upon Installation
In the 1.1 version, the Director icon would not appear in the Top Level NSX Collection Submap. This made it difficult to configure the Director using the GUI, and to see the hub and spoke topology representing deployed NSX's and Director. The Director icon now appears along with the NSX icons on the Top Level NSX Collection Submap. This icon allows users to view the current code version, to run nrConfigure on the Director.

nrConfigure Core Dump
The underlying UNIX socket interface library was receiving improperly formatted data. This formatting problem didn't allow a proper return status, which resulted in core dumps. To fix the bug, the library parameters were validated.

nrConfigure Variable Parameter Operations
There was a problem in which strings within quotes were not being interpreted as a single entity. nrConfigure now correctly parses these token strings.

Improved Installation

NetRanger 1.2 systems are now shipped with two new installation and configuration scripts: ***sysconfig-nsx*** and ***nrconfig***. sysconfig-nsx configures such basic NSX features as its IP address, COM serial ports, and so on. nrconfig configures NetRanger daemon services on Director as well as NSX systems.

NetRanger 1.1 Enhancements

This section identifies all of the major changes and enhancements associated with the 1.1 release of NetRanger. This information is presented within the context of the three main NetRanger systems: NSX, Communications, and Director.

NSX

Regular Expression Parsing

Content Signatures are now based on Regular Expressions rather than literal strings. In the 1.0 version of the NSX, sensord.conf contained multiple entries for a given string in order to account for such things as differences in case, leading and trailing spaces, and so on. The 1.1 version of the NSX is able to account for all of these variables through the use of regular expression syntax. For example, all combinations of "vrfy" attacks against the sendmail port can now be expressed simply as [Vv][Rr][Ff][Yy].

New Signatures

The following new attack signatures have been added into the NSX system: RPCs, DNS, WEB, YP, improved sendmail, TFTP, SYN denial-of-service, and TCP hijacking.

Communications

Sliding Window

NetRanger now uses a *sliding window* to send packets between post offices. This both improves both performance and reduces the number of packets that are dropped and must be retransmitted.

Failure Under Heavy Loads

Internal tests have shown that the 1.0 version of the communication system can fail with a *core dump* when subjected to heavy load. This has been fixed on the 1.1 release.

Director

Multiple and Read-Only Maps

With the 1.0 version of the Director, only one instance of the user interface could run concurrently. Version 1.1 allows multiple instances of the network management interface to run concurrently on the Director platform. An important benefit of this enhancement is that users at different locations can simultaneously view a common set of network security information.

Event Icon Consolidation

In the 1.0 version of the Director, the *nrdirmap* application displayed an icon for every alarm event it received. This quickly led to a cluttering of both the screen displays and the underlying OpenView object database. This is especially true when an NSX detects recurring events, such as ping sweeps from a specific IP address.

Version 1.1 of the Director contains the ability to consolidate duplicate alarms into a single icon and OpenView database entry. A counter on the icon indicates when a subsequent alarm of that type has been received. The threshold for consolidating duplicate alarms into a single icon/entry is configurable.

Remote Configuration

Users can now configure both local and remote NetRanger daemon applications via a Java-based configuration interface called **nrConfigure**. This interface is accessed from the Director via the **Security→Configure** menu option.

User-Defined Actions

In addition to displaying and logging alarm events, the 1.1 version of the Director can now generate user-defined actions via the *eventd* application. For example, *eventd* can generate pager notifications via e-mail for alarm events above a configurable threshold (e.g., level "4" alarms).

II NetRanger Pre-Installation

What to do Before Installing NetRanger 1.2

Before installing NetRanger, it is important to have a complete understanding of the current corporate network architecture. This is a critical step in the pre-installation process. Failure to obtain proper information could result in the creation of network security holes and loss of network functionality and services. This section describes what steps to take before installing the system on a network.

Analyze the Current Network Architecture

The first step in protecting a network is understanding the existing network architecture and requirements. The most effective way to analyze a network's current architecture is to follow these steps:

1. ***Identify what to protect.***
2. ***Define all entry and exit points to the protected network.***
3. ***Identify current security measures.***

Identify What to Protect

Think about which network assets need protection. Also, closely examine the connectivity *between* corporate networks that might give unwanted access to the network environment. If the configuration contains connections between more than one physical site, determine whether to protect the remote assets. If not, then determine whether to protect the network *from* the remote site.

Define All Entry and Exit Points to the Protected Network

This is the most important, and possibly the most difficult, step in protecting a network. The way an organization is connected physically as well as electronically affects identification of all network entry and exit points. Some typical scenarios follow.

Case 1—One Geographic Location, No Existing Internet Connection

This is the simplest case. If NetRanger is being installed at the same time an Internet connection is being established, then the NetRanger NSX can be installed as your Internet router as well as an intrusion detection and response system.

In order to isolate your internal network from other corporate networks as well as the Internet, identify all routers local to that network and either replace them with a NetRanger NSX or place a NetRanger NSX behind them. Refer to the *BorderGuard Setup* and *BorderGuard Configuration* sections in this *User's Guide* for detailed instructions on how to do this.

If your network connects to one or more business partner networks, security can be enhanced by placing a NetRanger NSX on that connection. It is difficult to control how a business partner's network is configured or what security countermeasures they have put in place to deter threats.

Case 2—One Geographic Location, Existing Internet Connection

In this situation, your organization has only one physical site, but more than one Internet connection. Each Internet connection must first be identified by contacting your Internet Service Provider to verify connectivity and registered Internet address ranges. Each registered address range assigned to your company should then be accounted for in the existing Internet router.

Refer to Case 1 for instructions on how to further secure your network.

Case 3—Multiple Geographic Locations, Existing Internet Connection

This is the most complicated situation. It is very likely that each site has its own Internet connection as well as a path to the network that needs protection. You have three options:

- **Protect your network at the Internet connection and at the connections to other sites**—This will secure all entry and exit points to your protected network. However, the remote sites will remain unprotected and the protected network will be more directly accessible to potential intruders.

- **Protect your local network and all remote network sites at their connections to the Internet**—This protects the corporate network from Internet intruders, but it does not secure communication between the corporate network and remote sites or business partners connected to your network.

- **Place NetRanger on all connections to the Internet, at connections to remote sites and at connections to business partners**—This provides the highest level of security and protects your network from internal as well as external (Internet) attacks.

Please note that the last two options require you to closely coordinate with network administrators at the remote sites to ensure complete coverage.

Identify Current Security Measures

How Existing Firewalls Affect NetRanger Installation

The NetRanger NSX can work in conjunction with existing firewalls as long as they are appropriately placed within your network. Ideally, the NetRanger NSX should be located *in front of* the existing firewall. If the NetRanger NSX packet filter is placed behind a firewall, intrusion detection will be limited to traffic that has been allowed through the firewall, and it will not generate alarms on reconnaissance or failed malicious activity. In cases where there is no need for address translation or other proxy services, NetRanger can replace firewalls. If there is no need for address translation or other proxy services, NetRanger works best without a firewall and has less impact on network performance.

How Security Filters in Existing Routers Impact NetRanger Installation

Please note that filters on existing routers must be removed for NetRanger to function **at its optimum level.** NetRanger will provide the same filtering capability in addition to its robust intrusion detection and response capabilities.

NSC BorderGuard Installation Options

Once your network architecture has been analyzed, the next step is to decide where to place the BorderGuard security device on the network. If you already have an established network, the simplest and least intrusive way to install the BorderGuard is as a **bridge device**. Otherwise, the simplest installation is to install the BorderGuard as a **router**. This section explains these as well as four other installation options. Please refer to the *BorderGuard Configuration* section for specific information about the configuration files for installing the BorderGuard.

Option 1—Install the BorderGuard as a Bridge

You will typically want to deploy the BorderGuard as a bridge when the network contains existing routers. In bridge mode, the BorderGuard can be placed in front of or behind your existing Internet router. It is usually simpler to place the BorderGuard on the LAN side. No subnetting of existing networks or additional networks is necessary. In most cases, the BorderGuard requires a single host address for configuration and VPN sleeves. Please note that when an NSX sensor and Director are directly connected to the BorderGuard (or they use an out-of-band channel), no IP address is needed. Thus NetRanger can be also installed in situations where there are *no* available IP addresses. The basic configuration for this installation option is diagrammed in Figure II-1.

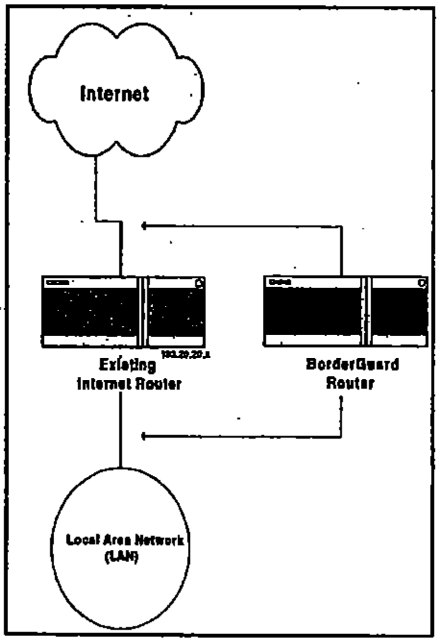


Figure II-1: BorderGuard Router in Bridge Mode

Option 2—Install the BorderGuard as the Internet Router

If your network has not yet been connected to the Internet, the simplest way to install the BorderGuard is as your Internet router. A BorderGuard 1000 or 2000 is usually connected to a Local Area Network (LAN) via Ethernet port(s). Connections to a CSU/DSU depends on the type of unit. Most CSU/DSU units have a V.35 serial connection; a small percentage use RS232 or RS449.

Your Internet Service Provider (ISP) assigns the external IP address, but all internal IP address(es) also need to be available for BorderGuard installation. If a connection to the Internet already exists, the current Internet router should be replaced and its IP address should be applied to the BorderGuard's external Ethernet. The basic configuration for this installation option is diagrammed in Figure II-2.

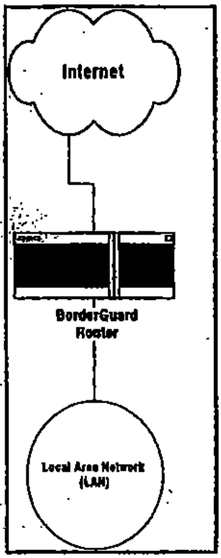


Figure II-2: The BorderGuard as the Internet Router

Options 3–6—Unable to Replace the Existing Internet Router

The remaining configuration options focus on situations where it is not possible or feasible to replace an existing Internet router with a BorderGuard unit (for example, an ISP may require a particular brand of router, such as a *Cisco*) and bridging is not desired. The following situations are discussed. You have:

- a class B address
- one or more unused class C addresses
- no unused class C addresses
- a class C address that cannot be subnetted

Option 3—A Class B Address

In this case, your Internet connection is based on a class B Internet address (the first number in the IP address is between 128 and 191, such as 130.130.x.x). An unused logical class C address can be assigned to the interface between the current router and the BorderGuard (such as 130.130.10.x). All current addresses can remain the same, and there is a minimal amount of overhead. This configuration is diagrammed in Figure II-3.

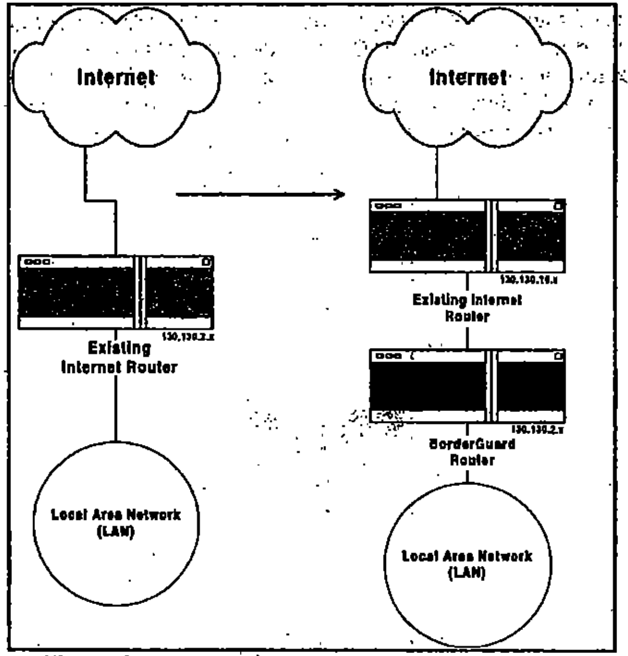


Figure II-3: BorderGuard Router Placed Behind the Existing Internet Router (Class B address space)

Option 4—An Unused Class C Address

Another option when the existing router cannot be replaced is to assign an unused class C address (the first number is greater than 191, such as 193.20.20.x) between the existing router and the BorderGuard. This can be done if multiple class C addresses exist and at least one of them is currently unused. As with Option 3, the remaining IP addresses can remain the same. This configuration is diagrammed in Figure II-4.

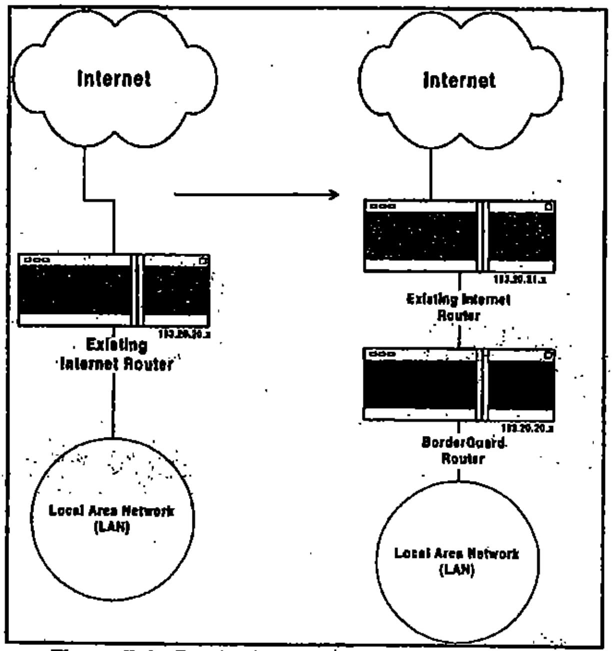


Figure II-4: BorderGuard Router Placed Behind the Existing Internet Router (Multiple Class C addresses)

Option 5—Unable to Replace Existing Internet Router and No Unused Class C Addresses

In some cases, it may not be possible to replace an existing Internet router and there are no unused class C addresses (the first number is greater than 191, such as 193.20.20.x). In this situation, subnet an existing class C network and change some internal host addresses. **Always try to subnet the class C address with the least number of hosts.** The addresses that must be changed are those that end in the first subnet range, such as x.x.x.1-31 for netmask 255.255.255.224, or those that end in the last subnet range, such as x.x.x.234-254 for netmask 255.255.255.224. This configuration is diagrammed in Figure II-5.

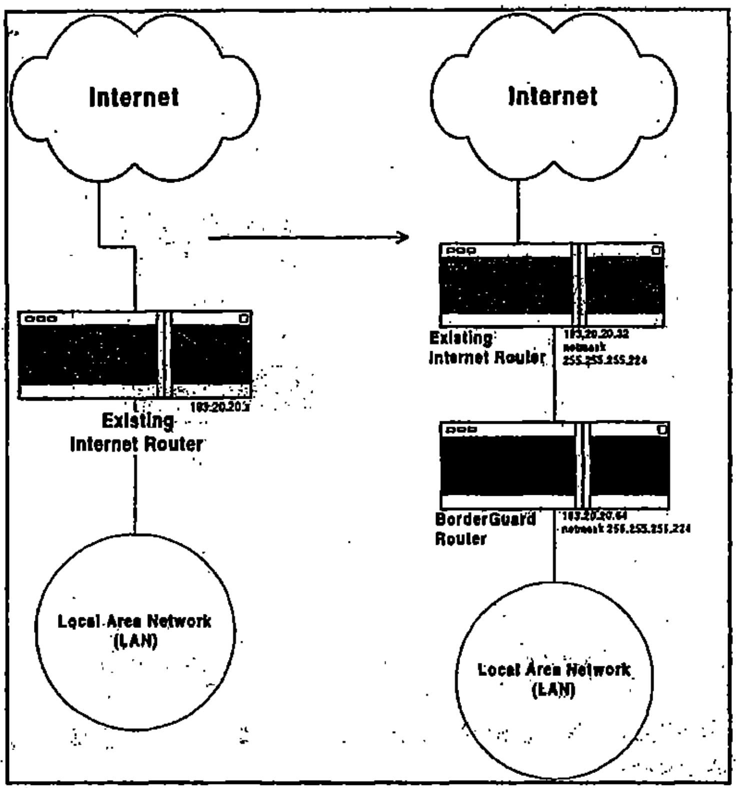


Figure II-5: BorderGuard Router Placed Behind the Existing Internet Router (Class C address is subnetted)

Option 6—Unable to Subnet The Existing Class C Address

In some cases, it is impossible to subnet a current class C address. This typically happens when only one registered class C address exists and all of its addresses are assigned. There are two options for installing the BorderGuard in this situation:

1. Obtain another class C address from the InterNic and employ Option 3 described earlier.
2. Purchase a proxy server or address translation device and remap the internal IP addresses.

The second option also requires that subnetting the class C address assigned to the BorderGuard router and the proxy server. While both of these options are fairly difficult, obtaining a new address is the least problematic of the two. These options are diagrammed in Figure II-6.

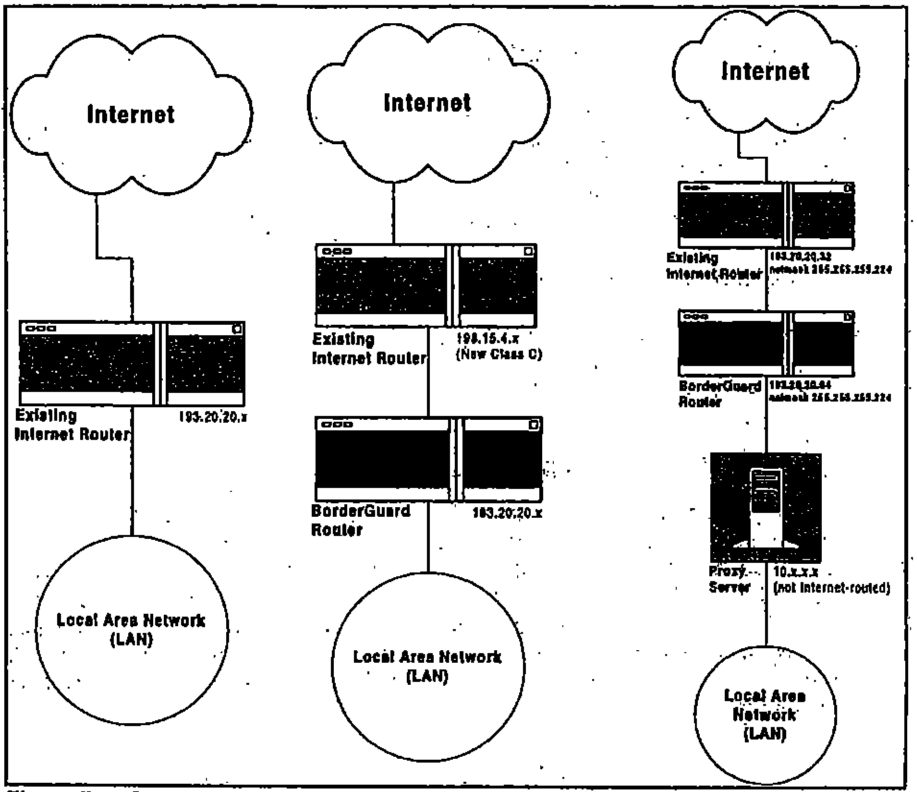


Figure II-6: BorderGuard Router Placed Behind the Existing Internet Router (Either assign a new class C address or use a proxy server for address translation)

NetRanger NSX Sensor Installation Options

In addition to determining how to deploy the BorderGuard, you will also need to consider the various options you have for placing the NSX sensor on your network. Each option carries with it different costs, such as extra ports on the BorderGuard; extra hardware (switched Ethernet hubs); and different benefits, such as increased security and performance. You can install the NSX sensor on your network in one of the following ways:

- install the NSX sensor on a separate, isolated network
- install the NSX sensor on the corporate network
- install the NSX sensor on a switched Ethernet network

Option 1—Install the NSX Sensor on a Separate, Isolated Network

The most secure NSX configuration is when the NetRanger NSX sensor is placed on its own network. This configuration can only be implemented with the NSX 2000 or 5000. Use one of the Ethernet interfaces on the BorderGuard 2000 to create a private network for the NSX sensor. The benefit of this configuration is that the traffic traveling between the BorderGuard and the NSX Sensor can be protected by the BorderGuard's security policy. This configuration also performs slightly better since communication between the BorderGuard and the NSX does not have to pass across your corporate network along with other traffic and is similar to the diagram illustrated in Figure II-7.

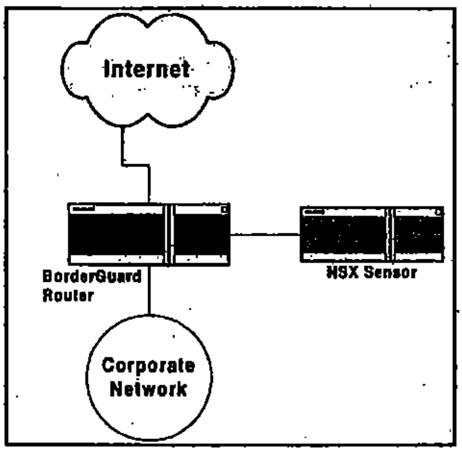


Figure II-7: The NSX Sensor Placed on its own Isolated Network

Option 2—Install the NSX Sensor on the Corporate Network

In this case, the NetRanger NSX sensor resides on the internal network. This configuration can be used with either the NSX 1000, 2000 or 5000. This configuration (which is diagrammed in Figure II-8) has two disadvantages:

- Communication between the BorderGuard and NSX sensor devices is mixed in with existing internal traffic and may create some overhead on the internal network.
- The NSX sensor is exposed to attacks from systems within the internal network. Unlike the first option, the BorderGuard filters cannot be used to protect the NSX sensor from these types of attacks

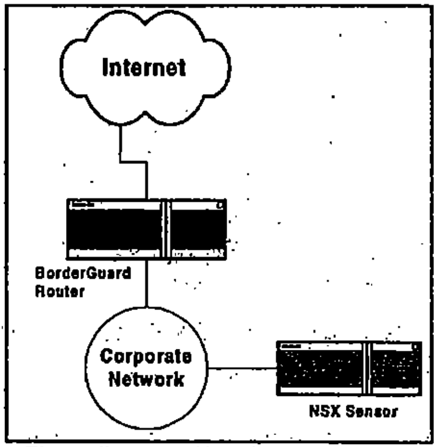


Figure II-8: The NSX Sensor Placed on the Corporate Network

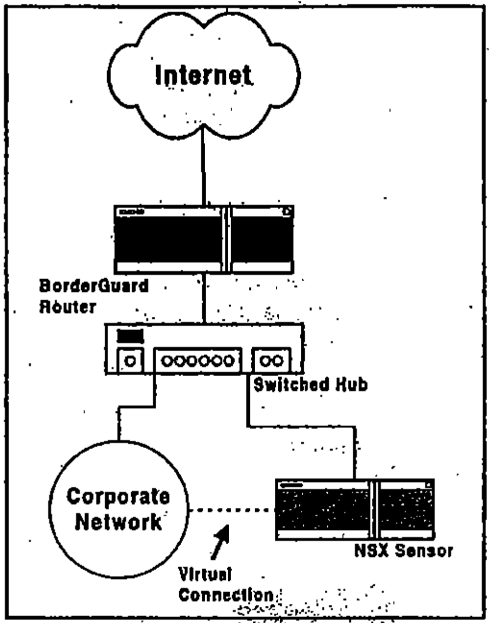


Figure II-9: The NSX Sensor Placed on a Switched Ethernet Network

Option 3—Install the NSX Sensor on a Switched Ethernet Network

With this option, the NetRanger NSX sensor resides on the same network as the rest of your users. The NSX Sensor is isolated from those users with a switched Ethernet hub, however. This configuration offers the same performance advantages as attaching the NSX Sensor directly to the BorderGuard, and it also provides additional security from the corporate network. The security won't be as robust as with Option 1, but the NSX Sensor traffic is protected from users on the internal network, which does provide some additional security. This configuration is diagrammed in Figure II-9.

NetRanger Director Setup Options

Two things must be considered when deciding where to place the NetRanger Director on your network. The first concerns operational use of the system. The Director should be placed in a physical location close to the individual(s) responsible for monitoring the networks. If X sessions will be used to access the Director, then it should be placed on the same network as the operators of that system. The second consideration relates to the Director's accessibility to NSX systems. There must be a path between the NSX and the Director for the alarm and management functions to work properly. If the Director is going to be placed on a network behind a proxy firewall or an address translation device, a NetRanger post office daemon must be loaded onto that device for communication to take place. Contact a WheelGroup representative for details on supported firewalls and operating systems.

Physical Installation Considerations

Because NetRanger is a significant component of the overall security environment, the NetRanger system(s) should be placed in a secure room. NSX and BorderGuard systems are shipped with rack mounts and can be located near other network equipment.

Power

Both the NSX and Director systems are currently UNIX-based and should be connected to an Uninterruptable Power Supply (UPS) to protect them from power outages and surges.

Physical and Operational Specifications

The BorderGuard 1000

Dimensions

- 2" high
- 19" wide (including rabbit ears)
- 17.5" deep
- weighs 15 pounds

Environment

- Operating Temperature—$^{+}$5º to $^{+}$45º C
- Storage Temperature— $^{-}$40º to $^{+}$70º C

Power Requirements

- AC Voltage/Frequency—110v/60Hz
- Power Supply Current—1.0 Amps (110)

Regulations (U.S.)

- UL1950, 1st edition

EMI/RFI

- FCC CFR 47 Part 15, Level B

The BorderGuard 2000

Dimensions

- 6.5" high
- 19" wide (including rabbit ears)
- 17.5" deep
- weighs 25 pounds

Environment

- Operating Temperature—$^{+}$5º to $^{+}$45º C
- Storage Temperature— $^{-}$40º to $^{+}$70º C

Power Requirements

- AC Voltage/Frequency—110v/60Hz; 230v/50Hz (switchable)
- Power Supply Current—1.5 Amps (110); 0.75 Amps (230)

Regulations (U.S.)

- UL1950, 1st edition

EMI/RFI

- FCC CFR 47 Part 15, Level B

The NSX Sensor

Dimensions

- 7" high
- 19" wide (including rabbit ears)
- 20" deep (including front handles)
- weighs 32 pounds

Environment

- Operating Temperature—$^{+}$10º to $^{+}$30º C
- Storage Temperature— $^{-}$40º to $^{+}$70º C

Power Requirements

- AC Voltage/Frequency—115v/60Hz; 230v/50Hz (switchable)
- Power Supply Current—1.5 Amps (110); 0.75 Amps (230)

Regulations (U.S.)

- UL1950, 1st edition

EMI/RFI

- FCC CFR 47 Part 15, Level B

Cabling and Setup

After the NSX Sensor has been configured, a terminal connection can be established between it and the BorderGuard router via a direct connect cable from the NSX serial port to the BorderGuard router console port. Refer to Table II-1 for the Cable and Ethernet transceiver type for your network connections. (The cable and Ethernet transceiver type will vary depending on the network connection.)

Cable Requirements

- The cable required for a BG1000-to-NSX connection is a 9-pinM to 9-pinF. (Attach a 9-pinM to the console port on the NSG and the 9-pinF to the serial port on the NSX.)

- The cable required for the BG2000-to-NSX connection is a 25-pinM to 9-pinF. (Attach a 25-pinM to the console port on the NSG and the 9-pinF to the serial port on the NSX.)

Initial Setup

To log into the BorderGuard Router after establishing the cable connection to the NSX Sensor, follow these steps:

1. **After attaching the console cable between the NSX Sensor and the BorderGuard Router, type the following at the NSX command line prompt:**

```
➤ tip hardwire2 <return>
```

2. **Type the password at the router password prompt. If no password has been set, press the Enter key to log onto the router.**

Interface	Connector
FDDI/single-mode FDDI	MIC / ST
IEEE 802.3/Ethernet	15-pin Ethernet AUI (10Base5)
MONITOR/MAINTENANCE ports	25-pin D-type, RS-232
Synchronous serial interface card	25-pin V.35, RS-422
Optical bypass Switch	6-pin DIN

Table II-1: Cable and Ethernet Transceiver Type for Network Connections

III Configuration and Installation

Installing and Configuring NetRanger 1.2

Proper installation of the NetRanger system involves the following steps, which are explained in this chapter:

- **Define the Security Policy**
- **Gather Network and Security Information**
- **Install and Configure the BorderGuard or Passport Security Device**
- **Install and Configure the NetRanger Director**
- **Install and Configure the NetRanger NSX Sensor**
- **Complete the nrconfig Utility Overview and Worksheets**

Define the Security Policy

Your security policy defines what type of activities and services you want to allow and disallow at key access points on your network. This includes

- services to allow **in** from untrusted sites,
- services to allow **out** from trusted sites (i.e., internal users), and
- **services you want to track**, such as Web traffic or FTP usage.

Implementation of your security policy is based largely on the filters installed on your BorderGuard or Passport security device. Use the following sections on **ICMP**, **TCP**, and **UDP** protocols as a guide to the configuration of the filter templates. Each section contains a subsection for **trusted and untrusted sites.** For more information on these services you may want to refer to such classic texts as *Internetworking With TCP/IP—Volume 1* by Douglas E. Comer (1995).

Gather Network and Security Information

Before installing and configuring the NetRanger system, you should gather the following information:

- BorderGuard/Passport IP addresses (One for each interface)
- NSX IP address
- Director IP address

- Internal Web server address
- Internal DNS server address
- Internal FTP server address

The following information should be available for each configured NetRanger NSX system:

ICMP (Internet Control Message Protocol)

ICMP allows routers and hosts to send error and control messages to other routers or hosts. One of the most frequent uses of this service is in support of the "ping" command, which queries a remote host or network device to see if it is alive on the network. This service is commonly used by hackers to discover potential targets by mapping out a remote network. It also allows internal users to check connectivity to a remote site. Use the following chart to help you map allowable ICMP messages.

Trusted: Enter "A" for *Allowed* or "B" for *Blocked* (the recommended entry is in parentheses). The number beside the Type Fields indicates the offset that will be required as part of a filter to block out this particular service (see the *Editing Default Filter Templates* section for more information).

Echo Reply: ________ (A)—Type Field (0)

Destination Unreachable ________ (A)—Type Field (3)

Source Quench ________ (A)—Type Field (4)

Redirect (change a route) ________ (A)—Type Field (5)

Echo Request ________ (A)—Type Field (8)

Time Exceeded for a Datagram ________ (A)—Type Field (11)

Parameter Problem on a Datagram ________ (A)—Type Field (12)

Timestamp Request ________ (A)—Type Field (13)

Timestamp Reply ________ (A)—Type Field (14)

Address Mask Request ________ (A)—Type Field (17)

Address Mask Reply ________ (A)—Type Field (18)

Untrusted: Enter "A" for *Allowed* or "B" for *Blocked* (the recommended entry is in parentheses). The number beside the Type Fields indicates the offset that will be required as part of a filter to block out this particular service (see the *Editing Default Filter Templates* section for more Information).

NOTE

All incoming requests to your network should be blocked.

Echo Reply: ________ (A)—Type Field (0)

Destination Unreachable ________ (A)—Type Field (3)

Source Quench ________ (A)—Type Field (4)

Redirect (change a route) ________ (A)—Type Field (5)

Echo Request ________ (B*)—Type Field (8)

Time Exceeded for a Datagram ________ (A)—Type Field (11)

Parameter Problem on a Datagram ________ (A)—Type Field (12)

Timestamp Request ________ (B*)—Type Field (13)

Timestamp Reply ________ (A)—Type Field (14)

Address Mask Request ________ (B*)—Type Field (17)

Address Mask Reply ________ (A)—Type Field (18)

NOTE

You may want to unblock services destined for your Internet servers such as a Web server, mail server, or FTP server. This function is explained in greater detail in the *Editing Default Filter Templates* section.

TCP (Transmission Control Protocol)

TCP is the most common transport layer protocol used on Ethernet and the Internet. Because of the connection-oriented characteristics of TCP, a connection is established every time a TCP service is used. Therefore, it is easy to ***block certain services from entering*** your network while at the same time ***allowing outgoing*** traffic. Use the following chart to help you map allowable TCP services. This list is not all-inclusive, but rather presents the most common TCP services that are included in the filter templates. Services that can be dynamically added to a filter have a corresponding entry in the NSX's *sensord.conf* file.

Trusted: Enter "A" for *Allowed* or "B" for *Blocked* (the recommended entry is in parentheses).

FTP Reply (Source Port 20*) ________ (B*)

FTP (Port 21) ________ (A)

Telnet (Port 23) ________ (A)

SMTP (Mail, Port 25) ________ (A)

DNS (Port 53) ________ (A)

Gopher (Port 70) ________ (A)

Finger (Port 79) ________ (A)

WWW (Port 80) ________ (A)

POP2 (Mail, Port 109) ________ (A)

POP3 (Mail, Port 110) ________ (A)

RPC (Port 111) ________ (A)

Auth (Port 113**) ________ (B)

NNTP (News Port 119) ________ (A)

NTP (Time Port 123) ________ (A)

Exec (Port 512) ________ (B)

Login (Port 513) ________ (B)

Cmd (Port 514) ________ (B)

Printer (Port 515) ________ (A)

ntalk (Port 518) ________ (A)

uucp (Port 540) ________ (A)

X11 (Ports 6000-6063***) ________ (B)

*A Source port of 20 should only be allowed on your trusted interface if you are maintaining an FTP server on your network. This port should be restricted to your FTP server.

**Connections outgoing to port 113 are usually initiated by mail or Web servers. These services request information from remote systems concerning the user who sent an e-mail or accessed a web page. The information that is received from the remote site is untrusted and is often used by hackers to "trick" your local system into performing actions under the hacker's direction. Unfortunately, you will need to allow this service because many mail servers require this service to operate. Upgrade or reconfigure your mail server as soon as possible, so that it no longer requires this service.

***Often when hackers break into remote systems, they initiate X sessions back to their remote site. For this reason, it is usually not advisable to allow outgoing X connections unless absolutely necessary.

Untrusted: Enter "A" for *Allowed* or "B" for *Blocked* (the recommended entry is in parentheses). Additional space after parenthesis is for the IP address(es) of the host you want to allow the service to.

DNS (Port 53) ________ (A*) ____________________

TFTP (Port 69) ________ (B) ____________________

RPC (Port 111) ________ (B) ____________________

NTP (Port 123) ________ (B) ____________________

Netbios (Ports 137-139) ________ (B) ____________________

SNMP (Ports 161,162) ________ (B) ____________________

Syslog (Port 514) ________ (B) ____________________

RIP (Port 520) ________ (B**) ____________________

Response ports (Ports > 1023) ________ (A***) ____________________

*You will typically want to restrict external access to a single DNS server.

**If using NetRanger between corporate partners or internal business networks, allow RIP or other routing protocols to pass. Work with the network administrator to determine which protocols need to be allowed.

***The only standard high-level UDP port usually allowed from an untrusted site is to a DNS server. Restrict it to that single IP address and to the UDP source port 53.

Install and Configure the BorderGuard

To install the BorderGuard, refer to the NSG BorderGuard Reference manual that corresponds to your unit.

Most of the settings required to deploy the BorderGuard or Passport are configured for you by the nrconfig script shipped with NetRanger under the /usr/nr/bin directory. In the event you need to manually edit any of these settings, please refer to Appendix B for manual configuration information. You can also refer to the NSG Reference manual that corresponds to your unit for additional information about these settings.

Install and Configure the NetRanger Director

Pre-Installation for HP-UX systems

Before you begin the installation process, verify that you meet the Software and Hardware Requirements listed below.

Software Requirements

You must have the following software either installed on your HP workstation or you must have the following software media and instructions:

- HP-UX 10.10 or greater
- HP OpenView 4.1 or greater

If you are installing the NetRanger Director on an HP workstation that already has HP-UX 10.10 or greater *and* HP OpenView 4.1 or greater installed, you can skip to the section entitled *Director Installation for HP-UX Systems.*

Hardware Requirements

The hardware requirements for the NetRanger/Director are dictated by the hardware requirements of HP OpenView. Consult the HP OpenView Installation documentation to ensure that your machine is powerful enough to run HP OpenView. In general, it is recommended that you use a dedicated machine that has at least 64 MB of RAM and at least 2 GB of disk space.

Installing HP-UX 10.10 or greater

Follow the directions in your HP-UX documentation to either install or upgrade to HP-UX 10.10.

8. **Uncompress these files using the following syntax (you must run this command for each of the five files):**

   ```
   uncompress <filename>
   ```

   Once the files are uncompressed, they should no longer have the ".Z" extension.

9. **Untar the uncompressed files, *except for the Java Development Kit*, using the following syntax:**

   ```
   tar -xvf <filename>
   ```

10. **Untar the Java Development Kit using the following commands:**

    ```
    mkdir -p /opt/SUNWjava

    cd /opt/SUNWjava

    tar -xvf /tmp/JDK_1_0_1-hpux10.tar

    mv JDK-1.0.1 JDK
    ```

11. **Run the install software by typing the following commands for each component:**

    Installing the NSX Interface software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCnsx WGCnsx
    ```

    Installing the DBMS software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCsapd WGCsapd
    ```

    Installing the Network Management Interface software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCdrctr WGCdrctr
    ```

    Installing the Remote Configuration software

    ```
    /usr/sbin/swinstall -v -x mount_all_filesystems=false -s /tmp/WGCcfgs WGCcfgs
    ```

12. **The Director installation process creates an account for the user "netrangr". You must set a password for that user. To set the password, type**

    ```
    passwd netrangr
    ```

13. **If *:/usr/nr/tmp* and *:/usr/nr/var* do not already exist, type the following command to create them:**

    ```
    mkdir /usr/nr/tmp

    mkdir /usr/nr/var
    ```

14. **If you would like the NetRanger daemons to start automatically at boot time, type:**

    ```
    /usr/nr/bin/install add
    ```

15. **Examine the file */tmp/nrdirmap.install.out* to ensure that no errors occurred.**

The installation is now complete. Go to the section entitled *Post-Installation for HP-UX and Sun Solaris Systems.*

Pre-Installation for Sun Solaris Systems

Before you begin the installation process, verify that you meet the Software and Hardware Requirements listed below.

Software Requirements

You must have the following software either installed on your Sun workstation or you must have the following software media and instructions:

- Solaris 2.4 or greater
- HP OpenView 4.1 or greater

If you are installing the NetRanger/Director on a Sun workstation that already has Solaris 2.4 or greater *and* HP OpenView 4.1 or greater installed, you can go to the section in this chapter entitled *Director Installation for Sun Solaris Systems.*

Hardware Requirements

The hardware requirements for the NetRanger/Director are dictated by the Hardware requirements of HP OpenView. Consult the HP OpenView Installation documentation to ensure that your machine is powerful enough to run HP OpenView. In general, it is recommended that you use a dedicated machine that has at least 64 MB of RAM and at least 2 GB of disk space.

Installing Solaris 2.4 or greater

Follow the directions in your Sun Solaris documentation to either install or upgrade to Solaris 2.4.

Installing HP OpenView 4.1 or greater on Solaris 2.4 or greater

1. **Before attempting to install HP OpenView, ensure that the following parameters are set correctly:**

- IP Address
- Hostname
- Subnet mask
- Default gateway IP Address
- Default gateway Hostname
- system time and timezone

2. **Reboot the machine. Once the machine has rebooted, you should be able to ping your loopback address, ping your IP address, resolve your loopback address, resolve your IP address, and resolve your hostname. Also, the timezone should be correct. Do not go to the next step until these TCP/IP parameters are properly configured.**

CAUTION

HP OpenView will not install correctly if TCP/IP is improperly configured.

3. **Install HP OpenView 4.1 or greater on the Sun Solaris machine (see the HP OpenView Installation Manual for details).**

CAUTION

- The HP OpenView installation will fail if semaphores are not enabled. Please refer to the section entitled Requirements for SunOS and Solaris Systems in the *HP OpenView Network Node Manager Products Installation Guide* to enable semaphores.
- HP OpenView 4.1.0 will not install on Solaris 2.5.x without an OpenView patch. Please contact your authorized HP representative to obtain this patch. (HP OpenView 4.1.1 and greater do not require this patch.)

5. **Add the following lines to the /.profile for user root. Please note the space between the "." and the "/":**

```
. /opt/OV/bin/ov.envvars.sh
export PATH=$PATH:$OV_BIN
```

Director Installation for Sun Solaris Systems

To install the NetRanger Director software on a Sun Solaris platform, follow these steps:

1. **Using** su, **log on as user root.**
2. **To load the OpenView environment variables, type the following command:**

```
. /opt/OV/bin/ov.envvars.sh
```

3. **If the OpenView user interface is running, stop it now by choosing** Map→Exit **from the OpenView menu. If other users have other copies of the user interface running and exported to other displays, ask them to shut down the user interface temporarily.**
4. **Put the NetRanger/Director tape in the tape drive if you have not already done so.**
5. **Go to the /tmp subdirectory by typing the following command:**

```
cd /tmp
```

6. **The NetRanger/Director install tape should contain compressed .tar files whose names have the following format:**

```
WGCnsx.<version>.<release>.<mod level>.<sys type>.tar.Z
WGCdrctr.<version>.<release>.<mod level>.<sys type>.tar.Z
WGCcfgs.<version>.<release>.<mod level>.<sys type>.tar.Z
WGCsapd.<version>.<release>.<mod level>.<sys type>.tar.Z
JDK-<version>_<release>_<mod level>-<sys type>.tar.Z
```

7. **Untar these files using the following syntax (you must run this command for each of the five files):**

```
tar -xvf /dev/rmt/0m <filename>
```

Where `<filename>` is the name of the compressed tar file.

8. **Uncompress these files using the following syntax (you must run this command for each of the five files):**

```
uncompress <filename>
```

Once the files are uncompressed, they should no longer have the ".Z" extension.

9. **Untar the uncompressed files, *except for the Java Development Kit*, using the following syntax:**

```
tar -xvf <filename>
```

10. **Untar the Java Development Kit using the following commands:**

```
mkdir -p /opt/SUNWjava
cd /opt/SUNWjava
tar -xvf /tmp/JDK-1_0_2-solaris2-sparc.tar
mv java JDK
cd /tmp
```

11. **Run the "package add" program by typing:**

```
pkgadd -d .
```

12. **Select the "WGCnsx" product from the "available packages" list.**
13. **Answer "yes" to the question about "install suid programs".**
14. **Answer "yes" to run the script as root.**
15. **Once the WGCnsx installation process has completed, select the "WGCdrctr" product from the "available packages" list.**
16. **Answer "yes" to any other questions the installation process might ask.**
17. **Select the "WGCcfg" product from the "available packages" list.**
18. **Answer "yes" to any other questions the installation process might ask.**

19. Select the "WGCsapd" product from the "available packages" list.
20. Answer "yes" to any questions the installation process might ask.
21. After the installation procedure is complete, type "q" to quit.
22. The Director installation process creates an account for the user "netrangr". You must set a password for that user. To set the password, type

    ```
    passwd netrangr
    ```

23. If */usr/nr/tmp* and */usr/nr/var* do not already exist, type the following to create them:

    ```
    mkdir /usr/nr/tmp
    mkdir /usr/nr/var
    ```

24. If you would like the NetRanger daemons to start automatically at boot time, type:

    ```
    /usr/nr/bin/install add
    ```

25. If this is a Solaris 2.4 installation, run the script below. If this is not a Solaris 2.4 installation, you do not need to run this script.

    ```
    /usr/nr/bin/postinstall.sh
    ```

26. Examine the file */tmp/nrdirmap.install.out* to ensure that no errors occurred.

The installation is now complete.

Post-Installation for HP-UX *and* Sun Solaris Systems—Cleanup

1. **As user root, start the HP OpenView daemons by typing the following:**

   ```
   $OV_BIN/ovstart
   ```

   If the ovstart executable is not found, then the `$OV_BIN` environment variable is probably not set properly in root's .profile. To set the variable, please refer to the step on loading the OpenView environment.

2. **To ensure that all OpenView daemons are running properly, type the following command:**

   ```
   $OV_BIN/ovstatus
   ```

3. **Remove all NetRanger Director tar files from the /tmp directory using the `rm` command.**

4. **From /tmp, remove the WGC directories by typing the following:**

   ```
   rm -rf WGC*.*
   ```

OPTIONAL

There is an OpenView daemon called *netmon* whose function is network mapping and availability monitoring. This daemon can be CPU-intensive. If you are only using OpenView to run the NetRanger Director, then it is not necessary to run this daemon.

To disable the *netmon* daemon, run the following commands:

```
$OV_BIN/ovstop netmon

$OV_BIN/ovdelobj $OV_LRF/netmon.lrf
```

5. **If necessary, set the DISPLAY variable in the appropriate `.profile` files.**

Configuring the User Environment

User netrangr uses the "ksh" Unix shell. The environment settings for user netrangr are kept in the file /usr/nr/.profile. The .profile puts /usr/nr/bin in the $PATH, and then it sets environment variables for OpenView, Java, and Oracle.

1. **To configure users other than "netrangr" to use the Director, ensure that the user uses "ksh". (This can be confirmed by viewing the `/etc/passwd` file.) and add the following lines from the /usr/nr/.profile to the user's $HOME/.profile:**

```
# Begin .profile additions
PATH=/usr/nr/bin:/usr/sbin:/usr/bin:/usr/ucb:/etc
export PATH
if [ -d /opt/OV ] ; then
        . /opt/OV/bin/ov.envvars.sh
        PATH=$OV_BIN:$PATH
        export PATH
        LD_LIBRARY_PATH=$OV_LIB:$LD_LIBRARY_PATH
        export LD_LIBRARY_PATH
fi

if [ -d /opt/SUNWjava ] ; then
        PATH=/opt/SUNWjava/JDK/bin:$PATH
        export PATH
        LD_LIBRARY_PATH=$HOME/lib:$LD_LIBRARY_PATH
        LD_LIBRARY_PATH=/opt/SUNWjava/JDK/lib/$sysType:$LD_LIBRARY_PATH
        export LD_LIBRARY_PATH
        CLASSPATH=$HOME/classes:/opt/SUNWjava/lib
        export CLASSPATH
fi
if [ -d /work/app/oracle ] ; then

        ORACLE_HOME=/work/app/oracle/product/7.3.2
        export ORACLE_HOME
        PATH=$PATH:$ORACLE_HOME/bin
        export PATH
        LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
        export LD_LIBRARY_PATH
fi

# End .profile additions
```

If the user must use a shell other than "ksh", then the lines above must be translated into the appropriate scripting language and placed in the appropriate shell startup file.

Post-Installation for HP-UX—*eventd* Configuration

If you plan to use the NetRanger *eventd* daemon, you should reconfigure the maximum number of processes that the HP Kernel will allow. Otherwise, if *eventd* receives a large number of alarm notifications in a short period of time, the likelihood that the number of processes executed by *eventd* could exceed the configured limits is increased.

To reconfigure the Kernel, follow these steps:

1. **As root, type:**

   ```
   sam &
   ```

2. **Choose** Kernel Configuration→Configurable Parameters.
3. **Highlight "nproc", then choose** Actions→Modify Configurable Parameters.
4. **Change the "Formula/Value" to the following:**

   ```
   (250+8*MAXUSERS)
   ```

5. **Press OK.**
6. **Highlight "maxuprc", then choose** Actions→Modify Configurable Parameters.
7. **Change the "Formula/Value" to the following:**

   ```
   300
   ```

8. **Press OK.**
9. **Choose** File→Exit.
10. **Choose OK to create the new Kernel and reboot the machine.**

Install and Configure the NetRanger NSX Sensor

Installing the NSX involves the following steps:

- Position the NSX in a stable location
- Attach power, network, and modem cables
- Initial access and NSX system configuration
- NetRanger-specific configuration

Position the NSX

The NSX should be placed in on a desk, shelf, equipment rack, wiring closet, or anywhere a computer may be safely placed. WheelGroup recommends that the NSX be placed physically close to the BorderGuard with which it will be operating. Ideally, the NSX should be placed within a standard communications rack.

Attach Power, Network, and Modem Cables

Proper installation of the NSX requires that the power cable and network cable to be installed. The NSX and BorderGuard should be plugged into an Uninterruptable Power Supply (UPS) to ensure continuous operation during power failures. The NSX is pre-configured to operate using the 10BaseT connector on the Ethernet card. Attachment of a modem cable to the internal modem is optional for most installations. However, this option is required only if initial configuration of the NSX will occur over a dial-up connection.

The NSX operating system is Solaris 2.5 x86. It is pre-installed on the internal hard disk along with the NetRanger software. The power to the NSX should never be turned off without first properly shutting down Solaris. Failure to do so may cause the file system on the NSX to become corrupted with possible loss of data. Prolonged exposure to repeated quick power-ons and power-offs may cause the NSX to not boot properly or not at all. If this occurs, please contact your NetRanger maintenance provider.

Initial Access and NSX System Configuration

The NSX may be initially configured by logging in through one of the following methods:

- console
- network
- serial
- modem

Network Access

The NSX login prompt may be accessed via the network. When you use this method of access, the login prompt will look similar to the example below. This requires attaching a computer to the same Ethernet LAN as the NSX and then using TELNET to connect to the NSX. The default IP address of the NSX is 10.1.9.201 with a netmask of 255.255.255.0. This requires that the computer used to access the NSX must be configured with an IP address of 10.1.9.1 through 10.1.9.254 excluding 10.1.9.201.

```
UNIX(r) System V Release 4.0 (nsx)

login:
```

Modem Access

The NSX login prompt may be accessed via the internal modem. When you use this method of access, the login prompt will look similar to the example below. This requires the installation of a standard telephone cable to the RJ-11 jack labeled TELCO located on the back of the NSX. The modem is configured to answer after the first ring. The NSX is pre-configured for a vt100 terminal once the modem connection is established.

```
modem login:
```

Serial Access

The NSX login prompt may be accessed via a serial connection to the COM1 port. When you use this method of access, the login prompt will look similar to the example below. This requires a null-modem cable to be attached between the NSX and a VT100-compatible terminal or a computer running terminal emulation software. Set the terminal or terminal emulation software to the following specifications:

```
Terminal:  VT100

Baud Rate:  9600

Word Length:  8 bit

Stop Bit: 1 bit

Parity:  No Parity
```

```
ttya login:
```

Console Access

The NSX login prompt may be accessed via the console. When you use this method of access, the login prompt will look similar to the example below. This requires the attachment of a keyboard and monitor to the NSX. A standard VGA-compatible monitor is adequate for access.

```
nsx console login:
```

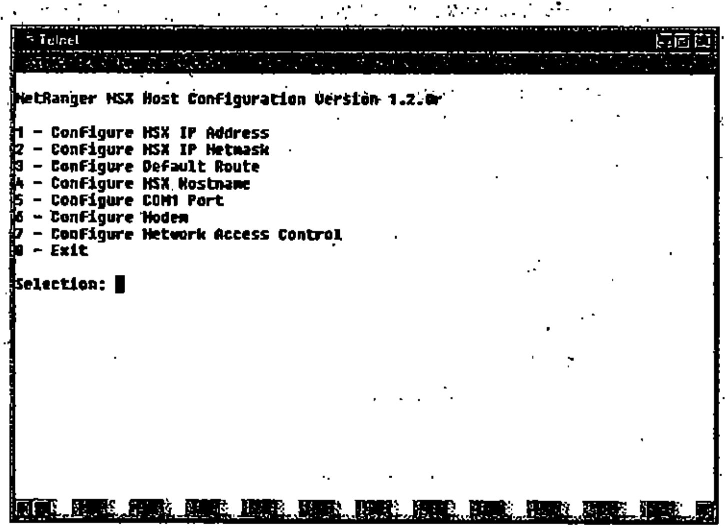
Logging In

Once the prompt is available, login as user *netrangr*. A password is not required, even though you will be prompted to set one. Once the initial prompt is accessed, use the su command to become the root user. The default root password is **`attack`**. Once the root prompt is accessed, immediately change the root password by using the **passwd** command.

NOTE

Write down the new passwords you have chosen for both *netrangr* and *root* and store them in a secure location.

As user *root*, access the host configuration utility to modify the IP address, IP netmask, hostname, and other configuration items for the NSX. The **`sysconfig-nsx`** command will display a menu, which is illustrated in Figure III-1 below, to select which items to configure.



```
NetRanger NSX Host Configuration Version 1.2.0

1 - Configure NSX IP Address
2 - Configure NSX IP Netmask
3 - Configure Default Route
4 - Configure NSX Hostname
5 - Configure COM1 Port
6 - Configure Modem
7 - Configure Network Access Control
0 - Exit

Selection: █
```

Figure III-1:NetRanger NSX Host Configuration Screen

Proper installation of the NSX requires that the IP address, IP netmask, and default route be configured. Be sure to configure the network access control to specify a list of IP addresses that require TELNET access to the NSX. The configuration utility only modifies the startup files for the operating system. The NSX will have to be rebooted for the new changes to take effect. Once configuration is complete, type in the command `init 6` to force the NSX to reboot.

NetRanger Specific Configuration

For information about configuring individual NSX machines, please refer to the following section which describes the nrconfig utility.

When you select a feature from the menu, it is prefixed by "ENABLED" to indicate that it is presently selected. To disable a selected feature, simply choose it from the menu again. The list of UNIX daemons required to support the "ENABLED" features is shown at the top of the screen above the Feature Selection menu.

To continue with NetRanger Configuration, choose **Enter** at the menu prompt. This takes you to the Main menu. You can return to this or any other menu at any time from the Main menu.

MAIN MENU

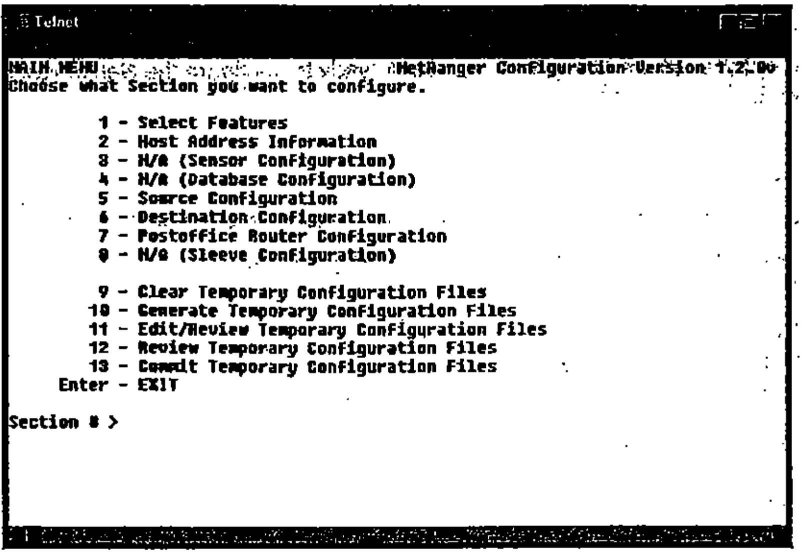
You can choose any of the following operations from the Main menu:

```
         1 - Select Features
         2 - Host Address Information
         3 - Sensor Configuration
         4 - Database Configuration
         5 - Source Configuration
         6 - Destination Configuration
         7 - Postoffice Router Configuration
         8 - Sleeve Configuration

         9 - Clear Temporary Configuration Files
        10 - Generate Temporary Configuration Files
        11 - Edit/Review Temporary Configuration Files
        12 - Review Temporary Configuration Files
        12 - Commit Temporary Configuration Files
     Enter - EXIT
```

Each menu item takes you through a series of configuration menus organized by feature requirements. Please note that features that are not required to support the specified NetRanger configuration are preceded by N/A (Not Available). For example, in the figure below, Sensor Configuration, Database Configuration, and Sleeve Configuration are Not Available in the Main Menu because the Director, Logging, Event Paging, and Postoffice Routing had been "ENABLED" in the Feature Selection menu. You can return to a configuration menu item at any time by selecting option 1 from the Main menu, even after exiting nrconfig, without losing any information that you may have already input.

Worksheets are provided on the following pages to help you organize your nrconfig information. Each Worksheet identifies the required features. If you have not "ENABLED" any of the corresponding features, you may skip the worksheets.



```
MAIN MENU                                   NetRanger Configuration Version 1.2.0b
Choose what Section you want to configure.

            1 - Select Features
            2 - Host Address Information
            3 - N/A (Sensor Configuration)
            4 - N/A (Database Configuration)
            5 - Source Configuration
            6 - Destination Configuration
            7 - Postoffice Router Configuration
            8 - N/A (Sleeve Configuration)

            9 - Clear Temporary Configuration Files
           10 - Generate Temporary Configuration Files
           11 - Edit/Review Temporary Configuration Files
           12 - Review Temporary Configuration Files
           13 - Commit Temporary Configuration Files
        Enter - EXIT

Section # >
```

1 - Select Features

This menu item takes you to the Feature Selection menu with which you were initially presented.

2 - Host Address Information

(Required for all Installations)

LOCAL HOST ADDRESS MENU

Enter this NetRanger's names and IDs in the following fields.

1 - **Organization Name** ____________________

2 - **Organization ID** ____________________

3 - **Host Name** ____________________

4 - **Host ID** ____________________

3 - Sensor Configuration

(Required for NSX)

This section establishes the IP addresses and netmasks for the BorderGuard's or Passport's Network Interfaces (The network device should separate your protected networks from outside untrusted networks.).

BorderGuard INTERFACES ENTRY MENU

> NOTE
>
> This is the first example of a configuration menu that allows a list of entries. You can add as many entries to the list as you can see on your screen. Each Entry menu allows you to Add, Edit, or Delete entries in the list.

Each entry contains the following three fields:

1 - **Interface Type (serial or ether)**

2 - **Interface IP Address**

3 - **PPP Destination IP Address or Interface Netmask**

Interface Type (serial or ether)	**IP Address**	**PPP Dest IP Address or NetMask**
serial / ether		
serial / ether		
serial / ether		
serial / ether		

Interface Type (serial or ether)—This defines whether the Interface is an Ethernet port or a serial port.

IP Address—This is the IP Address used by the BorderGuard **(serial)** for this PPP interface, or **(ether)** on the subnet connected to this interface.

PPP Destination IP Address or NetMask—This is the **(serial)** Destination IP Address used by the BorderGuard for this PPP interface, or the network **(ether)** IP mask used on the subnet connected to this interface.

BorderGuard CONFIGURATION MENU

Enter BorderGuard Configuration data into the following fields:

1 - **BorderGuard's Network Host Name** ______________________

2 - **BorderGuard's PASSWORD**______________________

3 - **BorderGuard's Version ID**______________________

4 - **BorderGuard's Primary IP Address**______________________

5 - **BorderGuard's External IP Address**______________________

6 - **BorderGuard's IP Address connected to NSX** ______________________

7 - **BorderGuard's default gateway** ______________________

8 - **NSX IP Address** ______________________

9 - **Minutes to log an event** ______________________

10 - **Minutes to shun an event** ______________________

BorderGuard's Network Host Name—This is the network host name for the BorderGuard used in /etc/hosts on the NSX or in DNS.

BorderGuard's PASSWORD—This is the password used to log into the BorderGuard.

BorderGuard's Version ID—This is the Version ID of the BorderGuard.

BorderGuard's Primary IP Address—The NetRanger system uses the Primary IP Address to establish encrypted sleeves and to communicate with the NSX. Ideally, this interface should be directly connected to the same LAN as the NSX.

NOTE

If you are using encrypted sleeves over the Internet, this should be a routeable Internet Address.

BorderGuard's External IP Address—The NetRanger uses the External IP Address as the connection to the untrusted networks.

BorderGuard's IP Address connected to NSX—This is the IP Address used by the BorderGuard on the subnet connecting the NSX to the BorderGuard.

BorderGuard's default gateway—This is the IP Address that the BorderGuard should use for its default gateway for IP packet routing.

NSX IP Address—This is the IP Address used by the NSX on the subnet connecting the NSX to the BorderGuard.

Minutes to log an event (optional)—This is the maximum number of minutes to log an event in an IP session.

Minutes to shun on an event (optional)—This is the maximum number of minutes to shun.

SECURITY POLICY CONFIGURATION MENU

This section establishes which incoming services to allow on your interface, and includes the servers through which this traffic will be allowed to pass. Enter the Server IP addresses for the allowed services into the following fields:

1 - External FTP Access Server ____________________

2 - External TELNET Access Server ____________________

3 - External MAIL Access Server ____________________

4 - External WEB Access Server ____________________

5 - External DNS Access Server ____________________

External FTP Access Server—This is the IP Address of the FTP Server that is allowed to service FTP requests coming in through the BorderGuard's External IP Address.

External TELNET Access Server—This is the IP Address of the TELNET Server that is allowed to service FTP requests coming in through the BorderGuard's External IP Address.

External MAIL Access Server—This is the IP Address of the SMTP Server that is allowed to service FTP requests coming in through the BorderGuard's External IP Address.

External WEB Access Server—This is the IP Address of the World Wide Web Server that is allowed to service FTP requests coming in through the BorderGuard's External IP Address.

External DNS Access Server—This is the IP Address of the DNS Server that is allowed to service FTP requests coming in through the BorderGuard's External IP Address.

STATIC ROUTES ENTRY MENU

This section establishes the IP Addresses, Netmasks, and Gateway IP Addresses for the Static Routes to be implemented by the BorderGuard. Each entry contains the following three fields:

1 - Network's IP Address

2 - Network's Netmask

3 - Network's Gateway IP Address

Network's IP Address	Network's Netmask	Network's Gateway IP Address

Network's IP Address—This is the IP Address for the subnet for the static route.

Network's Netmask—This is the netmask for the subnet.

Network's Gateway IP Address—This is the IP Address that acts as a gateway to the subnet for the static route.

INTERNAL NETWORKS ENTRY MENU

This section establishes the IP Addresses and Netmasks for the Internal Protected Networks. Each entry contains the following two fields:

1 - Network's IP Address

2 - Network's Netmask

Network's IP Address **Network's Netmask**

________________________ ________________________

________________________ ________________________

________________________ ________________________

________________________ ________________________

________________________ ________________________

Network's IP Address—This is the IP Address for the subnet for the internal network.

Network's Netmask—This is the netmask for the subnet.

4 - Database Configuration

(Required for Database)

DATABASE CONFIGURATION MENU.

Enter the Database User ID and Password for NetRanger into the following fields:

1 - Database USER ID ____

2 - Database PASSWORD ____

Database USER ID—This is the user id used to log into the database.

Database PASSWORD—This is the password used to log into the database.